Ne tak letmý úvod k maticím

První pracovní verze

Tento text na příkladech ukazuje vlastnosti základních algebraických struktur – grup, okruhů, polí, vektorových prostorů a algeber. Zvláštní důraz je kladen na vysvětlení operací v okruhu matic a dále na vysvětlení pojmů vektorového prostoru, vektorového podprostoru a lineárního zobrazení. V závěru je vysvětlena souvislost mezi soustavami homogenních lineárních rovnic, lineárními zobrazeními a podprostory.

Nejde o učebnici lineární algebry, takže některé důležité pojmy jsou opomenuty nebo není dostatečně vysvětlen jejich význam.

1. Matice a algebraické struktury

Definice. *Maticí typu $k \times l$ nad množinou S* rozumíme zobrazení

$$M : \{1, \dots, k\} \times \{1, \dots, l\} \to S.$$

Říkáme též, že matice M má k řádků a l sloupců. Hodnotě $M(i, j)$ říkáme *prvek matice M v i-tém řádku a j-tém sloupci*. Matice často zapisujeme prostřednictvím obdélníkové tabulky s k řádky a l sloupci. Poznamenejme, že v tomto textu v rozporu se zavedeným značením (ale v souladu s logiku edice *Letmý úvod*) nebudeme prvky matic značit malými písmeny.

Nyní ukážeme, že množiny matic mají určitou strukturu, aniž bychom přesně definovali, co se strukturou rozumí. Tento pojem však osvětlíme na řadě příkladů.

V množině přirozených čísel $\mathbb{N} = \{0, 1, \dots\}$ lze prvky sčítat a násobit. To znamená, že existují dvě *(binární) operace*, čímž rozumíme zobrazení

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$
$$\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}.$$

Píšeme ale pro přehlednost $a + b$ namísto $+(a, b)$ a podobně pro násobení.

Příkladem struktury je množina přirozených čísel s těmito dvěma (binárními) operacemi.

Odčítání ani dělení nejsou operacemi na $\mathbb{N}$, protože rozdíl nebo podíl dvou přirozených čísel nemusí být přirozené číslo.

Pokud chceme, aby odčítání byla operace, musíme rozšířit číselný obor, s nímž pracujeme. Dostaneme celá čísla $\mathbb{Z}$. Podobně se nám ale nepodaří rozšířit přirozená čísla na nějaký číselný obor, aby bylo operací i dělení – nulou dělit nejde.

Sčítání v $\mathbb{Z}$ je operace, která má tyto vlastnosti:

(1) $\forall a, b, c \in \mathbb{Z} : a + (b + c) = (a + b) + c$ (asociativita)

(2) $\exists 0 \in \mathbb{Z} \forall a \in \mathbb{Z} : 0 + a = a + 0 = a$ (existence neutrálního prvku)

(3) $\forall a \in \mathbb{Z} \exists b \in \mathbb{Z} : a + b = 0$ (existence inverzního prvku)

(4) $\forall a, b \in \mathbb{Z} : a + b = b + a$ (komutativita)

Definice. Řekneme, že množina S spolu s operací $\star$ je *grupa*, pokud splňuje vlastnosti 1–3, a *komutativní grupa*, pokud splňuje 1–4. Množinu S s operací $\star$ zapisujeme dvojicí $(S, \star)$.

Příklad 1. Tedy sčítání v $\mathbb{Z}$ je komutativní grupa. Sčítání v $\mathbb{N}$ vlastnosti komutativní grupy nemá a násobení v $\mathbb{N}$ ani v $\mathbb{Z}$ také ne. Povšimněte si ale, které z vlastností komutativní grupy násobení v $\mathbb{N}$ a v $\mathbb{Z}$ splňuje: je asociativní, existuje neutrální prvek a je komutativní. Kdybychom přidali zlomky a pracovali s racionálními čísly $\mathbb{Q}$, stejně nebude existovat inverzní prvek pro každé $a \in \mathbb{Q}$.

Násobení na $\mathbb{Q} - \{0\}$ je grupa.

Odčítání v $\mathbb{Z}$ není grupa. Také dělení v $\mathbb{Q}$ není grupa a ani v $\mathbb{Q} - \{0\}$ to není grupa.

Množina $\mathbb{Z}_3 = \{-1, 0, 1\}$ zbytkových tříd po dělení 3 je komutativní grupa vzhledem k operaci sčítání definované tabulkou

$+$	-1	0	1
-1	1	-1	0
0	-1	0	1
1	0	1	-1

Množina $S_0 = \{-1, 1\} \subseteq \mathbb{Z}$ s násobením definovaným stejně jako v $\mathbb{Z}$ je komutativní grupa. Povšimněte si, že $S_0 = \mathbb{Z}_3 - \{0\}$ – je to určitá analogie s $\mathbb{Q} - \{0\}$, která bude později důležitá.

Nyní se pokusíme definovat operace také na množinách matic. Označme

$$\mathrm{Mat}_{k\times l}(S) = \Big\{ M : \{1, \dots, k\} \times \{1, \dots, l\} \to S \Big\}$$

množinu všech matic typu $k \times l$.

Pokusme se definovat sčítání v $\mathrm{Mat}_{k\times l}(S)$ „po složkách“ předpisem

$$(M + N)(i, j) = M(i, j) + N(i, j),$$

kde $M, N \in \mathrm{Mat}_{k\times l}(S)$, $i = 1, \dots, k$, $j = 1, \dots, l$.

Uvědomte si, že tato definice nedává žádný smysl, protože v obecné množině S neumíme sčítat. V $\mathrm{Mat}_{k\times l}(\mathbb{N})$ jde ale o operaci.

Cvičení. Dokažte, že je-li $(G, +)$ grupa, je $\mathrm{Mat}_{k\times l}(G)$ s výše definovaným sčítáním také grupa, a je-li $(G, +)$ komutativní, je i $\mathrm{Mat}_{k\times l}(G)$ komutativní grupa.

Podobně jako sčítání lze v $\mathrm{Mat}_{k\times l}(\mathbb{N})$ definovat operaci násobení

$$(M * N)(i, j) = M(i, j) \cdot N(i, j).$$

Poznámka. Toto násobení nemá velké využití a to, že jej zde uvádíme, je matoucí a nepedagogické.

Cvičení. Rozhodněte, zda $\big(\mathrm{Mat}_{k\times l}(\mathbb{Z}), *\big)$, $\big(\mathrm{Mat}_{k\times l}(\mathbb{Q}), *\big)$ nebo $\big(\mathrm{Mat}_{k\times l}(\mathbb{Q}-\{0\}), *\big)$ jsou grupy, případně komutativní grupy.

Vraťme se nyní k celým číslům. Nic nám nebrání uvažovat operace sčítání a násobení současně. Víme, že $(\mathbb{Z}, +)$ je komutativní grupa a $(\mathbb{Z}, \cdot)$ nikoli. Platí však několik

vlastností, které svazují tyto dvě binární operace dohromady:

(5) $\forall a, b, c \in \mathbb{Z} : a \cdot (b + c) = a \cdot b + a \cdot c$ (levá distributivita)

(6) $\forall a, b, c \in \mathbb{Z} : (a + b) \cdot c = a \cdot c + b \cdot c$ (pravá distributivita)

Navíc, jak jsme již podotkli výše, je násobení v $\mathbb{Z}$ asociativní a komutativní a má neutrální prvek.

Definice. Množina S s dvěma (binárními) operacemi + a $\cdot$ se nazývá *okruh*, pokud $(S, +)$ je komutativní grupa, operace $\cdot$ je na S asociativní a má neutrální prvek a pokud + a $\cdot$ splňují 5–6. Je-li navíc $\cdot$ komutativní, mluvíme o *komutativním okruhu*.

Poznámka. Povšimněte si, že + v okruhu je podle naší definice komutativní vždy. Okruhy lze definovat obecněji, ale v našich úvahách to nebudeme potřebovat. Nekomutativní + vede k takovým komplikacím, že raději volíme méně obecnou definici.

Označení. V případě, že nemůže být pochyb o tom, které operace v grupách či okruzích uvažujeme, budeme místo označení grupy či okruhu používat pouze označení množiny bez operací. Budeme se snažit označovat abstraktní množiny písmenem S (set), grupy G a okruhy R (ring).

Neutrální prvek vzhledem k operaci + budeme označovat 0 a inverzní prvek vzhledem k + budeme nazývat opačný prvek. Neutrální prvek vzhledem k $\cdot$ budeme označovat 1. Tato konvence odpovídá označení prvků v číselných oborech, takže by neměla být příliš matoucí. Raději se zamyslete, zda vás v předchozím textu nemátlo, že např. neutrálním prvkem v grupě $(\mathbb{Q} - \{0\}, \cdot)$ byl prvek 1. Název inverzní prvek vyhradíme v okruzích pro inverzní prvek vůči $\cdot$.

Příklad 2. Příkladem okruhů je $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, nikoli $(\mathbb{Q} - \{0\}, +, \cdot)$. Okruhem je také $(\mathbb{Z}_3, +, \cdot)$, kde násobení je stejné jako v $\mathbb{Z}$.

Množina $\big(\mathrm{Mat}_{k\times l}(\mathbb{N}), +, *\big)$ okruhem není, ale $\big(\mathrm{Mat}_{k\times l}(\mathbb{Z}), +, *\big)$ a $\big(\mathrm{Mat}_{k\times l}(\mathbb{Q}), +, *\big)$ ano.

Dalším příkladem okruhu jsou polynomy $\mathbb{N}[x]$, $\mathbb{Z}[x]$ a $\mathbb{Q}[x]$ s koeficienty v množině přirozených, resp. celých a racionálních čísel. Operacemi na polynomech jsou běžné sčítání a násobení polynomů.

Ve všech příkladech okruhů jde o komutativní okruhy. S podstatným příkladem nekomutativního okruhu se setkáme v příkladu 25.

Povšimněte si, že některé okruhy se mírně liší od jiných v tom, jak „dobré“ je v nich násobení, resp. kolik prvků má inverzi vzhledem k násobení.

Definice. Nechť v komutativním okruhu $(R, +, \cdot)$ je splněna vlastnost

(7) $\forall r \in R, r \neq 0 \exists s \in R : r \cdot s = s \cdot r = 1$ (vlastnost pole)

Pak $(R, +, \cdot)$ nazýváme *pole*.

Poznámka. Je-li vlastnost 7 splněna v nekomutativním okruhu, nazýváme jej *těleso*. V dalším textu se však budeme věnovat výhradně polím, protože teorie těles je značně komplikovaná a nemá pro účely tohoto textu valný význam.

Příklad 3. Příkladem pole je $(\mathbb{Q}, +, \cdot)$ nebo $(\mathbb{Z}_3, +, \cdot)$. Žádný další okruh z uvedených příkladů polem není. Zamyslete se především, proč nesplňuje vlastnost 7 množina matic $\big(\mathrm{Mat}_{k\times l}(\mathbb{Q}), +, *\big)$. Toto je také patrně vhodné místo na to, abyste si připomněli, jak vypadají prvky 0 a 1 v maticích a jaké jsou tam opačné a inverzní prvky.

Cvičení. Dokažte tvrzení obsažená v předešlém příkladu.

Cvičení. Nechť v $(R, +, \cdot)$ platí silnější vlastnost než 7:

$$\forall r \in R \exists s \in r : r \cdot s = s \cdot r = 1.$$

Dokažte, že pak $R = \{1\}$ je tzv. *triviální okruh*, který není příliš zajímavý. To znamená, že vlastnost 7 není „slabá“ a definice pole je „rozumná“.

Poznámka. Pole pro nás budou důležitá později. Sluší se také vysvětlit, proč neuvádíme jako příklady polí další číselné obory, reálná a komplexní čísla. Důvodem je to, že z hlediska lineární algebry nepřináší tyto množiny nic podstatně odlišného od množiny racionálních čísel. Důvodem dalšího rozšiřování číselného oboru je buď snaha o metrickou úplnost, nebo o přidání kořenů polynomů vyššího řádu, což pro účely tohoto textu nemá žádný význam.

Grupy a okruhy představovaly struktury s (binárními) operacemi. Nyní se budeme věnovat strukturám zcela odlišným.

Uvědomte si, že pro $a \in \mathbb{Z}$ a polynom $p \in \mathbb{Q}[x]$ má smysl uvažovat polynom s racionálními koeficienty $a \cdot p$, čímž rozumíme pro $p = b_n x^n + \dots b_1 x + b_0$ polynom

$$a \cdot p = (a \cdot b_n)x^n + \cdots + (a \cdot b_1)x + (a \cdot b_0).$$

Toto násobení ale není v žádném případě binární operace, neboť mícháme prvky dvou různých množin. Formálně toto násobení představuje zobrazení, které pro větší přehlednost označíme jiným symbolem

$$\odot : \mathbb{Z} \times \mathbb{Q}[x] \to \mathbb{Q}[x].$$

Povšimněte si, že toto zobrazení splňuje

$$\forall p \in \mathbb{Q}[x] : 1 \odot p = p \qquad \text{(vlastnost jednotky)} \tag{8}$$

$$\forall a, b \in \mathbb{Z} \forall p \in \mathbb{Q}[x] : a \odot (b \odot p) = (a \cdot b) \odot p \qquad \text{(vnější asociativita)} \tag{9}$$

Povšimněte si vlastnosti 8. Zde 1 chápeme jako prvek $\mathbb{Z}$ a nikoli jako polynom nulového stupně z $\mathbb{Q}[x]$.

Poznámka. Nechť G je libovolná grupa a S libovolná množina. Pak zobrazení $G \times S \to S$ splňující 8 a 9 nazýváme *akce grupy G na množině S*. Akcím grup je z podstatné části věnován *Letmý úvod k afinním prostorům*, takže je nebudeme rozebírat příliš podrobně.

V našem případě jsou však $\mathbb{Z}$ a $\mathbb{Q}[x]$ okruhy a díky tomu má akce $\odot$ další významné vlastnosti:

$$\forall a \in \mathbb{Z} \forall p, q \in \mathbb{Q}[x] : a \odot (p + q) = a \odot p + a \odot q \quad \text{(levá vnější distributivita)} \tag{10}$$

$$\forall a, b \in \mathbb{Z} \forall p \in \mathbb{Q}[x] : (a + b) \odot p = a \odot p + b \odot p \quad \text{(pravá vnější distributivita)} \tag{11}$$

Cvičení. Pokuste se pochopit, která operace $+$ je na kterém místě ve vlastnostech 8–11 použita. V dalším textu budeme už opět pro jednoduchost označovat akci $\odot$ symbolem běžného násobení, takže si dobře rozmyslete vlastnost 9, kde vystupují oba tyto symboly.

Poznámka. Povšimněte si, že vlastnosti 8–11 nevyužívají toho, že $\mathbb{Q}[x]$ je okruh. Ve skutečnosti bychom tak měli mluvit o vlastnosti 9 jako o levé vnější asociativitě, přičemž pravá vnější asociativita by využívala násobení v $\mathbb{Q}[x]$. Vlastnosti formulované výše však užijeme v následující definici.

Definice. Nechť $(R, +, \cdot)$ je libovolný okruh a $(G, +)$ komutativní grupa. Nechť je definována akce $\odot : R \times G \to G$ splňující vlastnosti 8–11. Pak řekneme, že G *je modul nad* R, prvky R nazýváme *skaláry* a akci $\odot$ nazveme *vnější násobení* nebo též *násobení skalárem*.

Příklad 4. Také $\mathbb{Z}[x]$ je modul nad $\mathbb{Z}$, ale $\mathbb{Z}[x]$ není modul nad $\mathbb{Q}$. Povšimněte si, že také $\mathbb{Q}$ je modul nad $\mathbb{Z}$ a $\mathbb{Z}$ je modul nad $\mathbb{Z}$. To je příkladem hned dvou důležitých faktů.

Předně, každý okruh $(R, +, \cdot)$ je modulem nad $(R, +, \cdot)$, přičemž vnější násobení splyne s násobením $\cdot$.

Méně evidentní je druhé tvrzení: Každá komutativní grupa $(G, +)$ je modul nad $\mathbb{Z}$, přičemž operace $\odot : \mathbb{Z} \times G \to G$ je definována následovně. Nechť $g \in G$ je libovolné a $a \in \mathbb{Z}$ je kladné číslo, pak

$$a \odot g = g + g + \cdots + g,$$

kde g sečteme a-krát. Nechť $a = 0$, pak položme $a \odot g = 0 \in G$. Nechť konečně a je záporné, pak

$$a \odot g = (-g) + (-g) + \cdots + (-g),$$

kde $-g$ označuje inverzní prvek k g a sčítáme $(-a)$-krát.

Je přitom samozřejmé, že každý modul nad $\mathbb{Z}$ je zároveň komutativní grupou, tedy mezi komutativními grupami a moduly nad $\mathbb{Z}$ není žádný rozdíl.

Cvičení. Uvažte příklady různých okruhů a grup, s nimiž jsme se již setkali, a pokuste se rozhodnout, zda jsou některé z nich modulem nad některými z těchto okruhů. Především si všímejte maticových okruhů a grup.

Příklad 5. Označme symbolem $\mathbb{Q}[x]_n$ množinu všech polynomů stupně nejvýše n, tedy

$$\mathbb{Q}[x]_n = \{a_n x^n + \cdots + a_1 x + a_0; a_n, \ldots, a_0 \in \mathbb{Q}\}.$$

Tato množina je zřejmě komutativní grupou vzhledem k operaci sčítání. Je to tedy modul nad $\mathbb{Z}$. Je to ovšem také modul nad $\mathbb{Q}$. Na $\mathbb{Q}[x]_n$ lze definovat násobení podobně jako v případě zbytkových tříd $\mathbb{Z}_n$, ale tím se zabývat nebudeme. Pro naše účely jde o vhodný příklad modulu nad $\mathbb{Q}$.

Cvičení. Nechť $(R, +, \cdot)$ je okruh, $(G, +)$ komutativní grupa a $\odot : R \times G \to G$ definováno pro každé $r \in R$ a každé $g \in G$ předpisem $r \odot g = g$. Může být G modulem nad R vzhledem k tomuto vnějšímu násobení?

Příklad 6. Povšimněme si nyní rozdílu mezi moduly nad $\mathbb{Z}$ a moduly nad $\mathbb{Q}$. Víme již, že $\mathbb{Q}$ je modul nad $\mathbb{Z}$ i nad $\mathbb{Q}$. Chápejme nyní $\mathbb{Q}$ jako modul nad $\mathbb{Q}$ a zvolme libovolně nenulový skalár $p \in \mathbb{Q}$ a prvek $q \in \mathbb{Q}$. Pak zřejmě existuje skalár $p^{-1} \in \mathbb{Q}$ tak, že

$$q = (p^{-1} \cdot p) \cdot q = p^{-1} \cdot (p \cdot q).$$

Nyní ale chápejme $\mathbb{Q}$ jako modul nad $\mathbb{Z}$ a zvolme libovolný nenulový skalár $a \in \mathbb{Z}$. Pak ale

$$q = (a^{-1} \cdot a) \cdot q = a^{-1} \cdot (a \cdot q)$$

jen v těch případech, kdy existuje inverzní prvek k a, tedy pouze tehdy, je-li $a = \pm 1$.

Definice. Modul nad polem nazýváme *vektorový prostor*. Prvky vektorového prostoru nazýváme *vektory*.

Označení. Abstraktní pole budeme označovat symbolem $\mathbb{K}$ a budeme mluvit o vektorových prostorech nad polem $\mathbb{K}$.

Poznámka. Vektorové prostory jsou základním pojmem lineární algebry. Prostor, který jim věnujeme v tomto textu, pochopitelně není dostatečný. Doporučujeme proto důkladné studium tohoto pojmu v některé z učebnic, např. [H] nebo [S].

Příklad 7. Grupy $\mathbb{Q}$, $\mathbb{Q}[x]$ a $\mathbb{Q}[x]_n$ jsou vektorovými prostory nad polem $\mathbb{Q}$. Grupa matic $\mathrm{Mat}_{k\times l}(\mathbb{Q})$ je vektorový prostor nad $\mathbb{Q}$. Obecně každé pole je vektorovým prostorem nad sebou samým. Množina $\{0\}$ je vektorový prostor nad každým polem.

Pojem vektorového prostoru se může na první pohled zdát poněkud zbytečným. Oproti modulům nad obecným okruhem však máme možnost formulovat některé důležité pojmy.

Definice. Řekneme, že množina vektorů $S \subseteq V$ je *lineárně nezávislá*, pokud pro každou její konečnou podmnožina $\{v_1, \ldots, v_k\} \subseteq S$ a každou množinu skalárů $\{a_1, \ldots, a_k\}$ platí, že

$$a_1 \cdot v_1 + \cdots + a_k \cdot v_k = 0 \qquad \Longrightarrow \qquad a_1 = \cdots = a_k = 0.$$

Řekneme, že množina je *lineárně závislá*, pokud není lineárně nezávislá.

Příklad 8. Množina $\{0\} \subseteq V$ je vždy lineárně závislá, obecněji každá množina vektorů obsahující nulový vektor je lineárně závislá. Jednoprvková množina $\{v\}$, kde $v \in V$ je nenulový vektor, je vždy lineárně nezávislá.

Příklad 9. Označme $\mathbb{Z}_6 = \{0, 1, \ldots, 5\}$ a definujme sčítání a násobení na $\mathbb{Z}_6$ následovně: nechť pro $a, b \in \mathbb{Z}_6$ je $a + b$ rovno zbytku po dělení 6 ze součtu $a + b$ v $\mathbb{N}$, podobně nechť $a \cdot b$ je rovno zbytku po dělení 6 ze součinu $a \cdot b$ v $\mathbb{N}$. Takto je např. $4 + 3 = 1$ nebo $2 \cdot 5 = 4$. Lze snadno ukázat, že $(\mathbb{Z}_6, +, \cdot)$ je okruh. Z příkladu 4 víme, že každý okruh je modulem sám nad sebou. Přitom $\mathbb{Z}_6$ není pole, neboť jen 1 a 5 má v $\mathbb{Z}_6$ inverzi. Tedy $\mathbb{Z}_6$ není vektorový prostor nad $\mathbb{Z}_6$.

Srovnejte to se $\mathbb{Z}_3$, které je vektorovým prostorem nad $\mathbb{Z}_3$. (Lze ukázat, že $\mathbb{Z}_n$ je pole právě tehdy, když n je prvočíslo.)

Uvažme nyní množinu $\{2\} \subseteq \mathbb{Z}_6$. Protože $3 \cdot 2 = 0$, vidíme, že na rozdíl od vektorových prostorů může být jeden prvek modulu lineárně závislý. Tedy v modulech nemusí mít pojem lineární nezávislosti smysl.

Příklad 10. Ve skutečnosti byl hlavní problém předchozího příkladu v tom, že v $\mathbb{Z}_6$ existují tzv. *dělitelé nuly*, tedy nenulové prvky, které lze vynásobit vhodným nenulovým prvkem tak, že výsledkem je nula. Uvědomte si, že např. v $\mathbb{Z}$ dělitelé nuly nejsou. Okruhu bez dělitelů nuly říkáme *obor integrity*. V modulech nad oborem integrity má lineární závislost a nezávislost smysl, nicméně záhy dospějeme k dalšímu pojmu, který ukáže, proč je výhodnější pracovat s vektorovými prostory.

Definice. Nechť V je vektorový prostor nad $\mathbb{K}$ a $v_1, \dots, v_k \in V$. Nechť $a_1, \dots, a_k \in \mathbb{K}$. Výraz tvaru

$$a_1 \cdot v_1 + \cdots + a_k \cdot v_k$$

nazveme *lineární kombinací vektorů* $v_1, \dots, v_k$.

Poznámka. Platí zřejmě $0 \cdot v_1 + \cdots + 0 \cdot v_k = 0$ pro libovolné vektory $v_1, \dots, v_k$. Lineární kombinaci s nulovými skaláry říkáme *triviální lineární kombinace*. To tedy znamená, že vektory $v_1, \dots, v_k$ jsou lineárně nezávislé právě tehdy, je-li každá jejich netriviální lineární kombinace různá od nuly.

Poznámka. Lineární kombinace jsou jen konečné součty. To plyne z toho, že operace součtu více vektorů je vlastně definována pomocí indukce, tedy pro $v_1, \dots, v_n \in V$ musíme chápat $v_1 + \cdots + v_n$ jako $v_1 + (v_2 + (\cdots + (v_{n-1} + v_n) \dots)$, přičemž na uzávorkování nezáleží, neboť sčítání je asociativní. Jinak řečeno, díky tomu, že umíme sečíst dva vektory, umíme jich sečíst konečně mnoho.

Protože často pracujeme s nekonečnými množinami, nabízí se chybná představa, že i operace mohou být nekonečněkrát opakovány. Už v nejjednodušším příkladu vektorového prostoru $\mathbb{Q}$ nad $\mathbb{Q}$ dobře víme, že nekonečný součet racionálních čísel není racionální číslo, ale nějaká podivná nekonečná řada.

Promyslete si, zda podobnou chybu neděláte při práci s libovolnými operacemi, nejen s lineárními kombinacemi ve vektorovém prostoru.

Příklad 11. Nechť $v_1, \dots, v_k \in V$ jsou lineárně závislé. Pak lze některý z vektorů $v_1, \dots, v_k$ vyjádřit jako lineární kombinaci ostatních. Skutečně, je-li

$$a_1 \cdot v_1 + \cdots + a_k \cdot v_k = 0$$

pro vhodné skaláry a $a_i \neq 0$ pro některé $i = 1, \dots, k$, pak

$$v_i = a_i^{-1} \cdot (a_1 \cdot v_1 + \cdots + a_{i-1} \cdot v_{i-1} + a_{i+1} \cdot v_{i+1} + \cdots + a_k \cdot v_k).$$

Uvědomte si, že ne každý vektor v_i lze takto vyjádřit, neboť je-li příslušný skalár a_i roven nule, neexistuje k němu inverzní prvek.

Rozmyslete si pečlivě situaci, kdy je jediný skalár v lineární kombinaci nenulový.

Příklad 12. Povšimněte si, že toto tvrzení neplatí v modulech nad obory integrity, protože ne každý nenulový prvek oboru integrity má inverzní prvek. Nechť $\mathbb{Z}$ je vektorový prostor nad $\mathbb{Z}$. Pak 2 a 3 jsou lineárně závislé, protože $-3 \cdot 2 + 2 \cdot 3 = 0$, ale 3 nelze vyjádřit jako lineární kombinaci 2 a naopak. (Lineární kombinace jednoho vektoru je jeho skalární násobek.) Pokud ale budeme 2 a 3 chápat jako prvky vektorového prostoru $\mathbb{Q}$ nad polem $\mathbb{Q}$, lze 2 vyjádřit snadno jako $2 = 2/3 \cdot 3$ a podobně $3 = 3/2 \cdot 2$. Pokud ale chápeme 2 a 3 jako prvky modulu $\mathbb{Q}$ nad okruhem $\mathbb{Z}$, jsme ve stejné situaci, jako by šlo o prvky $\mathbb{Z}$.

Definice. Nechť V je vektorový prostor nad $\mathbb{K}$ a $S \subseteq V$ libovolná podmnožina. *Lineárním obalem množiny* S nazveme množinu

$$\mathrm{Lin}(S) = \{a_1 \cdot v_1 + \cdots + a_k \cdot v_k; k \in \mathbb{N}, a_1, \ldots, a_k \in \mathbb{K}, v_1, \ldots, v_k \in S\},$$

je-li $S \neq \emptyset$, lineární obal prázdné množiny $\mathrm{Lin}(\emptyset)$ klademe roven $\{0\}$. Množinu S nazýváme *množinou generátorů* prostoru V, pokud $\mathrm{Lin}(S) = V$.

Příklad 13. Povšimněte si především, že každý vektorový prostor je množinou generátorů sebe sama.

Definice. Lineárně nezávislá množina generátorů se nazývá *báze*.

Poznámka. Povšimněte si, že množinou generátorů vektorového prostoru $\{0\}$ je prázdná množina. Ta je jistě lineárně nezávislá, tedy je to báze $\{0\}$.

Příklad 14. Pojem lineárního obalu má smysl i pro moduly. Uvažme $\mathbb{Z}$ jako modul nad $\mathbb{Z}$. Množina $\{2, 3\}$ je množinou generátorů. Jiným příkladem je množina $\{1\}$. Zatímco $\{1\}$ je lineárně nezávislá množina (a tedy „báze“ v $\mathbb{Z}$), množina $\{2, 3\}$ je lineárně závislá.

Věta. *Je-li množina generátorů vektorového prostoru V konečná, lze z ní vybrat bázi.*

Důkaz. Důkaz provedeme indukcí vzhledem k počtu generátorů. Vektorový prostor $\{0\}$ má prázdnou bázi. V příkladu 8 jsme viděli, že jednoprvková množina generátorů je lineárně nezávislá, tedy báze.

Nechť věta platí pro $k - 1$ generátorů a nechť $V = \mathrm{Lin}(\{v_1, \ldots, v_k\})$. Pokud jsou generátory lineárně nezávislé, jsme hotovi, pokud ne, lze podle příkladu 11 některý generátor, řekněme v_1, vyjádřit jako lineární kombinaci ostatních.

Pak ale $V = \mathrm{Lin}(\{v_2, \ldots, v_k\})$ a podle indukčního předpokladu lze vybrat bázi. □

Poznámka. Povšimněte si, že tvrzení platí pouze pro konečnou množinu generátorů. Kdyby toto omezení v předpokladech věty nebylo, šlo by vybrat bázi ze všech prvků vektorového prostoru vzhledem k příkladu 13. Věta tedy neříká, že má každý vektorový prostor bázi. Ve skutečnosti je existence báze nekonečněrozměrného vektorového prostoru ekvivalentní s axiomem výběru.

Příklad 15. Vraťme se k příkladu 14. Z množiny $\{2, 3\}$ nelze vybrat bázi, protože ani 2, ani 3 negenerují celé $\mathbb{Z}$ (například jimi nelze vygenerovat prvek 1).

Příklad 16. Chápejme $\mathbb{Q}$ jako vektorový prostor nad $\mathbb{Q}$. Pak je každá jednoprvková množina $\{q \in \mathbb{Q}; q \neq 0\}$ báze v $\mathbb{Q}$. Obecněji, chápeme-li pole $\mathbb{K}$ jako vektorový prostor nad $\mathbb{K}$, je množina $\{k \in \mathbb{K}; k \neq 0\}$ jeho bazí.

Množina $\{1, x, x^2, \ldots, x^n, \ldots\}$ je bazí v $\mathbb{Q}[x]$, podobně $\{1, x, \ldots, x^n\}$ je bazí v $\mathbb{Q}[x]_n$.

Nechť $O_{i,j}$ označuje matici typu $k \times l$ definovanou předpisem

$$O_{i,j}(p, q) = \begin{cases} 1 \text{ pro } p = i, q = j \\ 0 \text{ jinak} \end{cases}$$

Pak množina $\{O_{i,j};\ i = 1, \ldots, k,\ j = 1, \ldots, l\}$ je bazí v $\mathrm{Mat}_{k \times l}(\mathbb{K})$.

Cvičení. Dokažte všechna tvrzení z předešlého příkladu.

Příklad 17. Příklad 11 lze nahlédnout ještě z jiné strany. Nechť $\{v_1, \dots, v_k\} \subseteq V$ je lineárně nezávislá množina a $u \in \mathrm{Lin}(\{v_1, \dots, v_k\})$. Pak množina $\{u, v_1, \dots, v_k\}$ je lineárně závislá, neboť

$$u = a_1 \cdot v_1 + \cdots + a_k \cdot v_k$$

pro vhodné skaláry a tedy

$$(-1) \cdot u + a_1 \cdot v_1 + \cdots + a_k \cdot v_k = 0.$$

Nechť nyní specielně $\{v_1, \dots, v_n\} \subseteq V$ je báze a $u \in V$ libovolný vektor. Protože báze generuje V, platí $u \in \mathrm{Lin}(\{v_1, \dots, v_n\})$. To ale znamená, že u je lineární kombinací vektorů báze, tedy

$$u = a_1 \cdot v_1 + \cdots + a_n \cdot v_n.$$

Je toto vyjádření jednoznačné? Kdyby existovaly skaláry $b_1, \dots, b_n \in \mathbb{K}$ tak, že

$$u = b_1 \cdot v_1 + \cdots + b_n \cdot v_n,$$

pak by platilo

$$a_1 \cdot v_1 + \cdots + a_n \cdot v_n - (b_1 \cdot v_1 + \cdots + b_n \cdot v_n) = (a_1 - b_1) \cdot v_1 + \cdots + (a_n - b_n) \cdot v_n = 0,$$

protože jsou ale vektory $v_1, \dots, v_n$ lineárně nezávislé, znamená to, že $a_i = b_i$ pro $i = 1, \dots, n$.

2. Vektorové prostory a matice přechodu

Označení. Z praktických důvodů budeme nadále pracovat nikoli s bázemi jako množinami, ale jako s uspořádanými n-ticemi, což se občas nazývá *uspořádané báze*. My nicméně budeme říkat pouze báze a budeme velmi volně nakládat s tím, kdy myslíme bazí uspořádanou a kdy neuspořádanou množinu a necháme na čtenáři, aby rozdíl vyrozuměl z kontextu. Báze budeme zapisovat jako řádky a označovat malými písmeny řecké abecedy.

Definice. Nechť $\alpha = (v_1, \dots, v_n)$ je báze V nad $\mathbb{K}$ a $u \in V$ libovolný vektor. Pak podle příkladu 17 existují jednoznačně určené skaláry $a_1, \dots, a_n \in \mathbb{K}$ tak, že

$$u = a_1 \cdot v_1 + \cdots + a_n \cdot v_n.$$

Tyto skaláry budeme nazývat *souřadnice vektoru u vzhledem k bázi α* a zapisovat jako sloupec

$$(u)_\alpha = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

Příklad 18. Povšimněte si především, že pro každou bázi $\alpha = (v_1, \dots, v_n)$ ve V platí

$$(v_1)_\alpha = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \quad (v_2)_\alpha = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \quad \dots \quad (v_{n-1})_\alpha = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}, \quad (v_n)_\alpha = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

Příklad 19. Mějme dvě báze, např. $\alpha = (1, x, x^2, \ldots, x^n)$ a $\beta = (1, 1+x, 1+x+x^2, \ldots, 1+x+\cdots+x^n)$ v $\mathbb{Q}[x]_n$. Uvědomte si, že podle příkladu 17 lze každý vektor báze β jednoznačně vyjádřit jako lineární kombinace vektorů z α a také naopak. Přesvědčte se o tom a souřadnice jednotlivých bázových vektorů vypočtěte.

Uvažme bázi $\gamma = (1+x, x+x^2, x^2+x^3, \ldots, x^{n-1}+x^n)$. Jako cvičení vyjádřete každý z vektorů γ v souřadnicích vzhledem k α a β. Jde to i naopak?

Neměli byste být překvapeni, že nikoli. Vektor 1 totiž není v $\mathrm{Lin}(\gamma)$, tedy γ není báze. Povšimněte si především, že zatímco α a β jsou $(n+1)$-tice vektorů, je γ jen n-tice. Znamená to tedy, že báze musí mít stejný počet prvků?

Lemma. *Nechť $\alpha = (v_1, \ldots, v_n)$ je báze V nad $\mathbb{K}$ a $u \neq 0$ libovolný vektor. Pak existuje $i = 1, \ldots, n$ takové, že $(u, v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$ je báze V.*

Důkaz. Protože α je báze, platí $u \in \mathrm{Lin}(\alpha)$, přesněji

$$u = a_1 \cdot v_1 + \cdots + a_n \cdot v_n.$$

Nechť $a_i \neq 0$, pak

$$v_i = a_i^{-1}(u - a_1 \cdot v_1 - \cdots - a_{i-1} \cdot v_{i-1} - a_{i+1} \cdot v_{i+1} - a_n \cdot v_n). \tag{12}$$

Nechť $w \in V$ je libovolný vektor. Dosadíme do lineární kombinace

$$w = b_1 \cdot v_1 + \cdots + b_n \cdot v_n$$

za v_i vyjádření 12. Tím jsme ale vyjádřili vektor w jako lineární kombinaci množiny $\{u, v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n\}$, tedy $\{u, v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n\}$ generuje V.

Kdyby nyní byla $\{u, v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n\}$ lineárně závislá množina, znamenalo by to, že $u \in \mathrm{Lin}(\alpha - \{v_i\})$. Vzhledem k 12 by ale pak také $v_i \in \mathrm{Lin}(\alpha - \{v_i\})$ a α by nebyla báze, což není možné.

Tedy $(u, v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$ je báze V. □

Věta (Steinitz)**.** *Nechť $\alpha = (v_1, \ldots, v_n)$ je báze V nad $\mathbb{K}$ a $\{u_1, \ldots, u_k\}$ je lineárně nezávislá množina vektorů. Pak $k \leq n$ a mezi vektory báze existuje taková $(n-k)$-tice $v_{i_1}, \ldots, v_{i_{n-k}}$, že $(u_1, \ldots, u_k, v_{i_1}, \ldots, v_{i_{n-k}})$ je báze V.*

Důkaz. Důkaz provedeme indukcí vzhledem ke k s využitím předešlého lemmatu, které představuje první krok.

Nechť $k \leq n$ a věta platí pro $k-1$, tedy platí, že $(u_1, \ldots, u_{k-1}, v_{i_1}, \ldots, v_{i_{n-k+1}})$ je báze V. Pak ale

$$u_k = a_1 \cdot u_1 + \cdots + a_{k-1} \cdot u_{k-1} + a_k \cdot v_{i_1} + \cdots + a_n \cdot v_{i_{n-k+1}}.$$

Kdyby $a_j = 0$ pro $j \geq k$, znamenalo by to, že množina $\{u_1, \ldots, u_k\}$ není lineárně nezávislá, protože

$$a_1 \cdot u_1 + \cdots + a_{k-1} \cdot u_{k-1} + (-1) \cdot u_k = 0.$$

To ale odporuje předpokladům, tedy některé a_j pro $j \geq k$ je nenulové. Nyní můžeme stejně jako v lemmatu nahradit $v_{i_{j-k}}$ vektorem u a dostaneme bázi.

Zbývá ukázat, že k nemůže být větší než n. Vzhledem k tomu, že v n-tém indukčním kroku obdržíme bázi $(u_1, \ldots, u_n)$, musela by být množina $\{u_1, \ldots, u_k\}$ lineárně závislá. □

Důsledek. *Má-li vektorový prostor konečnou bázi, mají všechny jeho báze stejný počet prvků.*

Definice. Nechť V je vektorový prostor. Mohutnost báze nazveme *dimenzí vektorového prostoru* V.

Poznámka. V definici báze stojí proti sobě dva principy. Báze je množina generátorů, ale zároveň je lineárně nezávislá. Generátorů musí být „dost“, lineárně nezávislých vektorů nesmí být „zbytečně mnoho“. Báze je minimální množina generátorů a zároveň maximální lineárně nezávislá množina.

Příklad 20. Nyní se vraťme k definici souřadnic a k zápisu bazí a souřadnic do řádků a sloupců. Nechť ve vektorovém prostoru V nad polem $\mathbb{K}$ je báze $\alpha = (v_1, \dots, v_n)$ a nechť $u \in V$ je vektor se souřadnicemi

$$(u)_\alpha = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

To znamená, že

$$u = a_1 \cdot v_1 + \cdots + a_n \cdot v_n.$$

Tuto lineární kombinaci budeme symbolicky zapisovat

$$u = \alpha \cdot (u)_\alpha \tag{13}$$

a chápat $\cdot$ jako určitou operaci. V striktně algebraickém smyslu to operace není, není to ani akce nebo něco podobného.

Povšimněte si zejména, že pomocí zápisu 13 lze přepsat lineární nezávislost vektorů báze α formálně výrazem

$$\forall c \in \mathrm{Mat}_{n\times 1}(\mathbb{K}) : \alpha \cdot c = 0 \implies c = 0. \tag{14}$$

Podívejme se na „násobení“ v 13 blíže. Zde je situace komplikovaná tím, že mícháme dohromady různé věci – vektory a skaláry. Zkoumejme proto jednodušší situaci. Nechť R je libovolný okruh. Maticím $\mathrm{Mat}_{1\times n}(R)$ říkejme *n-řádky* a maticím $\mathrm{Mat}_{n\times 1}(R)$ podobně *n-sloupce*. Nechť M je n-řádek a N je n-sloupec, definujme jejich *součin* jako $a \in R$,

$$a = \sum_{i=1}^{n} \big(M(1,i) \cdot N(i,1)\big).$$

Součin n-řádku s n-sloupcem je tedy zobrazení

$$\cdot : \mathrm{Mat}_{1\times n}(R) \times \mathrm{Mat}_{n\times 1}(R) \to R.$$

Poznámka. Nyní se nabízí otázka, proč raději nepsat báze i souřadnice oboje do řádků (či sloupců) a nedefinovat součin pro dva stejně dlouhé řádky či dva stejně dlouhé sloupce. Odpověď bude pochopitelná po určitém zobecnění součinu řádků se sloupci. Další vtíravá otázka, proč nepsat naopak souřadnice do řádků a matice do sloupců, bude vysvětlena o něco později.

Příklad 21. Povšimněme si nyní dvou bazí, např. bazí α a β v $\mathbb{Q}[x]_n$ z příkladu 19. Vezměme si po řadě souřadnice vektorů z α vzhledem k bázi β, tedy

$$(1)_\beta = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad (x)_\beta = \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad (x^2)_\beta = \begin{pmatrix} 0 \\ -1 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \ldots, \quad (x^n)_\beta = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ -1 \\ 1 \end{pmatrix}.$$

Pokud postupně aplikujeme na bázi β a jednotlivé sloupce součin 13, dostaneme vektory báze α.

Sestavme nyní z těchto sloupců čtvercovou matici a definujme další součin, opět obecně pro matice nad okruhem R. Nechť M je n-řádek a $N \in \mathrm{Mat}_{n\times n}(R)$, jejich součinem nazveme n-řádek P splňující pro každé $i = 1, \ldots, n$ vztah

$$P(1, i) = M \cdot N(-, i).$$

Symbolem $N(-, i)$ zde myslíme i-tý sloupec N a součin na pravé straně rovnosti je tedy součin n-řádku s n-sloupcem. Poznamenejme, že podobně budeme symbolem $X(i, -)$ označovat i-tý řádek matice X, podtržítko zde znamená prázdné místo, do něhož lze dosazovat, tedy formálně je

$$N(-, i) : \{1, \ldots, n\} \to R, \qquad \Big(N(-, i)\Big)(j) = N(j, i).$$

Povšimněte si, že součin n-řádku s maticí $n \times n$ odpovídá tomu, jak jsme vyjádřili bázi α z báze β. Tam jsme vlastně násobili takto:

$$\alpha = \beta \cdot \Big(\ (1)_\beta \mid (x)_\beta \mid \ldots \mid (x^n)_\beta \ \Big),$$

přičemž symbolem vpravo rozumíme matici $n \times n$ vzniklou tak, že sloupce napíšeme vedle sebe, tedy

$$\Big(\ (1)_\beta \mid (x)_\beta \mid \ldots \mid (x^n)_\beta \ \Big)(-, i) = (x^{i-1})_\beta.$$

Povšimněme si nyní velmi důležité věci. Nechť $u \in \mathbb{Q}[x]_n$. Pak

$$u = \alpha \cdot (u)_\alpha = \left(\beta \cdot \Big(\ (1)_\beta \mid (x)_\beta \mid \ldots \mid (x^n)_\beta \ \Big)\right) \cdot (u)_\alpha. \tag{15}$$

Definujme další součin, velmi podobný jako předešlý. Nechť M je matice $n \times n$ a N je n-sloupec. Jejich součinem nazveme n-sloupec P splňující pro $i = 1, \ldots, n$

$$P(i, 1) = M(i, -) \cdot N.$$

Pak lze výraz 15 přepsat jako

$$u = \alpha \cdot (u)_\alpha = \beta \cdot \left(\Big(\ (1)_\beta \mid (x)_\beta \mid \ldots \mid (x^n)_\beta \ \Big) \cdot (u)_\alpha\right)$$

a vzhledem k jednoznačnosti souřadnic vzhledem k dané bázi to znamená, že

$$(u)_\beta = \Big(\ (1)_\beta \mid (x)_\beta \mid \ldots \mid (x^n)_\beta \ \Big) \cdot (u)_\alpha$$

Poznámka. Poznamenejme, že jsme v předchozím příkladu několikrát aplikovali nově definované součiny v situacích, kdy řádkem nebyl n-řádek, ale uspořádaná báze. V těchto případech jsme však k součinu přistupovali jako k výrazu 13.

Definice. Nechť $\alpha = (v_1, \dots, v_n)$ a β jsou báze ve vektorovém prostoru V. Čtvercovou matici $(\mathrm{id})_{\beta\alpha}$ splňující

$$(\mathrm{id})_{\beta\alpha}(-, i) = (v_i)_\beta,$$

tedy

$$(\mathrm{id})_{\beta\alpha} = \big(\ (v_1)_\beta \ \big|\ (v_2)_\beta \ \big|\ \dots \ \big|\ (v_n)_\beta\ \big)$$

nazýváme *matice přechodu od báze α k bázi β*.

Poznámka. Uvědomte si, že vzhledem k jednoznačnosti souřadnic je také matice přechodu určena jednoznačně. Označení matice přechodu bude jasné později, povšimněte si obráceného pořadí bazí v indexu $(\mathrm{id})_{\beta\alpha}$.

Příklad 22. Nyní ukážeme motivaci pro definování dalšího součinu. Nechť α, β a γ jsou tři báze ve V. Nový součin bude definován tak, že matice přechodu od α ke γ bude součinem matice přechodu od β ke γ s maticí přechodu od α k β.

Nechť tedy M a N jsou matice $n \times n$. Jejich součinem nazveme matici P typu $n \times n$ splňující pro $i = 1, \dots, n$ a $j = 1, \dots, n$ vztah

$$P(i, j) = M(i, -) \cdot N(-, j),$$

tedy v i-tém řádku a j-tém sloupci součinu je součin i-tého řádku M s j-tým sloupcem matice N.

Vraťme se k motivaci. Víme, že pro každé $u \in V$ je

$$u = \alpha \cdot (u)_\alpha = \gamma \cdot (\mathrm{id})_{\gamma\alpha} \cdot (u)_\alpha.$$

Zároveň ale

$$u = \alpha \cdot (u)_\alpha = \beta \cdot (\mathrm{id})_{\beta\alpha}(u)_\alpha = \gamma \cdot (\mathrm{id})_{\gamma\beta} \cdot (\mathrm{id})_{\beta\alpha} \cdot (u)_\alpha$$

Protože matice přechodu je dána jednoznačně, musí platit

$$(\mathrm{id})_{\gamma\alpha} = (\mathrm{id})_{\gamma\beta} \cdot (\mathrm{id})_{\beta\alpha}.$$

Součin na pravé straně je pak právě součin čtvercových matic definovaný výše.

Poznámka. Uvědomte si, že součin čtvercových matic je operace z algebraického hlediska, neboť je to zobrazení

$$\cdot : \mathrm{Mat}_{n\times n}(R) \times \mathrm{Mat}_{n\times n}(R) \to \mathrm{Mat}_{n\times n}(R).$$

Příklad 23. Součin matic $n \times n$ je asociativní operace, neboť pro každé $M, N, P \in \mathrm{Mat}_{n\times n}(R)$ je

$$\Big((M \cdot N) \cdot P\Big)(i, j) = \big(M \cdot N\big)(i, -) \cdot P(-, j) = M(i, -) \cdot N \cdot P(-, j)$$

a naopak

$$\Big(M \cdot (N \cdot P)\Big)(i, j) = M(i, -) \cdot \big(N \cdot P\big)(-, j) = M(i, -) \cdot N \cdot P(-, j)$$

Ujistěte se, že dobře rozumíte výše uvedenému zápisu. Uvědomte si také, že ze zápisu plyne, že i-tý řádek součinu matic M a N je součinem i-tého řádku M s maticí N. Promyslete si, jak tento fakt plyne z definice násobení n-řádku maticí $n \times n$ (viz příklad 21). Dále si rozmyslete podobný fakt pro sloupce.

Poznámka. V poznámce k příkladu 20 jsme se zamýšleli nad tím, proč nedefinovat součin n-řádku s n-řádkem či naopak n-sloupce s n-sloupcem. Nyní, když znáte součin čtvercových matic, se můžete zamyslet, s jakými obtížemi by se definoval součin matic, pokud bychom chtěli vyjít např. od součinu n-řádků. Uvažme takový součin „po řádcích“. Především vůbec není jasné, který prvek ve výsledné matici kam psát, na rozdíl od součinu, který jsme definovali my. Připusťme ale, že bychom zavedli nějakou konvenci, např. takovou, že v i-tém řádku a j-tém sloupci součinu je součin i-tého řádku s j-tým řádkem, tedy např. u matic 2×2 dostaneme

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bf & ag+bh \\ ce+df & cg+dh \end{pmatrix}.$$

Takový součin ale nebude asociativní! Vyzkoušejte

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix}$$

a okamžitě vidíte, že v prvním řádku prvním sloupci výsledné matice je při jednom uzávorkování $aei+bfi+agj+bhj$ a při druhém $aei+afj+bek+bfl$.

Promyslete si dobře, že asociativitu nezískáte ani při jiné konvenci uspořádání prvků. Formální důkaz tohoto tvrzení by byl zdlouhavý a nebudeme jej uvádět.

Cvičení. Ověřte, že matice E_n typu $n \times n$ definovaná předpisem

$$E_n(i,j) = \begin{cases} 1 \text{ pro } i = j \\ 0 \text{ jinak,} \end{cases}$$

je jednotkovým prvkem vzhledem k násobení matic $n \times n$.

Poznámka. Z příkladu 18 plyne, že pro každou bázi α ve vektorovém prostoru V dimenze n je $(\mathrm{id})_{\alpha\alpha} = E_n$.

Příklad 24. Vraťme se na chvíli k násobení řádků sloupci. Násobení n-řádku n-sloupcem je zleva i zprava distributivní operace, což plyne přímo z distributivity násobení v R. Přesněji, pro libovolné $M, N \in \mathrm{Mat}_{1\times n}(R)$ a $P, Q \in \mathrm{Mat}_{n\times 1}(R)$ platí

$$\begin{aligned} M \cdot (P+Q) &= \sum_{i=1}^{n} M(1,i) \cdot \big(P(i,1) + Q(i,1)\big) \\ &= \sum_{i=1}^{n} \big(M(1,i) \cdot P(i,1) + M(1,i) \cdot Q(i,1)\big) = M \cdot P + M \cdot Q \end{aligned}$$

a podobně

$$(M+N)\cdot P = \sum_{i=1}^{n} \big(M(1,i)+N(1,i)\big)\cdot P(i,1)$$
$$= \sum_{i=1}^{n} \big(M(1,i)\cdot P(i,1) + N(1,i)\cdot P(i,1)\big) = M\cdot P + N\cdot P$$

Především z toho plyne, že pro libovolnou lineární kombinaci vektorů $v_1,\dots,v_k \in V$ a libovolnou bázi α ve V platí

$$(c_1\cdot v_1 + \cdots + c_k\cdot v_k)_\alpha = c_1\cdot (v)_1 + \cdots + c_k\cdot (v)_k.$$

Nechť nyní $A,B,C \in \mathrm{Mat}_{n\times n}(R)$. Protože součin čtvercových matic je definován tak, že v i-tém řádku a j-tém sloupci matice $A\cdot B$ je součin i-tého sloupce A s j-tým sloupcem B, plyne z distributivity násobení řádků sloupci také

$$A\cdot(B+C) = A\cdot B + A\cdot C$$
$$(A+B)\cdot C = A\cdot C + B\cdot C.$$

Důsledek. *Z úvah v předchozích dvou příkladech a z předchozího cvičení vyplývá, že* $(\mathrm{Mat}_{n\times n}(R),+,\cdot)$ *tvoří okruh, přičemž nulová matice* 0_n *je nulový prvek a jednotková matice* E_n *je jednotkový prvek.*

Poznámka. Zdůrazněme, že tento okruh je podstatně významnější než výše uvedený okruh $(\mathrm{Mat}_{n\times n}(R),+,*)$ s násobením po složkách, jehož zavedení nemělo jiný smysl než ilustrovat na příkladech pojem okruhu.

Příklad 25. Nechť V je vektorový prostor nad polem $\mathbb{K}$ dimenze n Nechť α, β jsou libovolné báze. Pak vzhledem k příkladu 18 a z jednoznačnosti matice přechodu plyne

$$(\mathrm{id})_{\beta\alpha}\cdot(\mathrm{id})_{\alpha\beta} = (\mathrm{id})_{\beta\beta} = E_n$$

a tedy $(\mathrm{id})_{\beta\alpha}$ je inverzní prvek k $(\mathrm{id})_{\alpha\beta}$ vzhledem k násobení matic. Specielně to znamená, že každá matice přechodu má inverzní prvek.

Tedy množina matic přechodu tvoří grupu vzhledem k násobení, nazývá se *obecná lineární grupa* a značíme ji $GL(n,\mathbb{K})$. Tato grupa není komutativní, např.

$$\begin{pmatrix}1&2\\3&4\end{pmatrix}\cdot\begin{pmatrix}1&1\\1&2\end{pmatrix} = \begin{pmatrix}3&5\\7&11\end{pmatrix}$$
$$\begin{pmatrix}1&1\\1&2\end{pmatrix}\cdot\begin{pmatrix}1&2\\3&4\end{pmatrix} = \begin{pmatrix}4&6\\7&10\end{pmatrix}$$

To především znamená, že $(\mathrm{Mat}_{n\times n}(\mathbb{K}),+,\cdot)$ není komutativní okruh a že obecněji pro libovolné R okruh $(\mathrm{Mat}_{n\times n}(R),+,\cdot)$ není komutativní.

Jak ale ukázat, že výše uvedené matice jsou skutečně maticemi přechodu? Existují vůbec nějaké matice typu $n\times n$, které by nebyly maticemi přechodu?

Především lze ukázat, že pro libovolné n nemá nulová matice 0_n inverzní prvek. Skutečně, pro každé $M\in\mathrm{Mat}_{n\times n}(\mathbb{K})$ je

$$0_n\cdot A = A\cdot 0_n = 0_n.$$

Protože už víme, že každá matice přechodu má inverzní prvek, nemůže být nulová matice maticí přechodu.

Poznámka. Podobně jako $GL(n, \mathbb{K})$ v $(\mathrm{Mat}_{n\times n}(\mathbb{K}), +, \cdot)$ je v každém okruhu množina prvků, které mají inverzi (tzv. *invertibilních prvků*) grupou vzhledem k násobení. Připomeňme, že v netriviálním poli je jediným prvkem bez inverze nulový prvek. Naopak např. v $\mathbb{Z}$ jsou invertibilními prvky pouze 1 a -1. V dalším textu budeme postupně směřovat k tomu, zda je invertibilních matic (tedy matic přechodu) spíše „málo“ podobně jako v $\mathbb{Z}$, nebo „většina“ podobně jako v poli.

Cvičení. Nechť M a N jsou matice přechodu. Dokažte, že pak

$$(M \cdot N)^{-1} = N^{-1} \cdot M^{-1}.$$

Příklad 26. Buď $\alpha = (v_1, \ldots, v_n)$ báze V. Označme

$$\begin{aligned}
\beta &= (v_1, \ldots, v_{i-1}, v_j, v_{i+1}, \ldots, v_{j-1}, v_i, v_{j+1}, \ldots, v_n),\\
\gamma &= (v_1, \ldots, v_{i-1}, v_i + v_j, v_{i+1}, \ldots, v_n),\\
\delta &= (v_1, \ldots, v_{i-1}, a \cdot v_i, v_{i+1}, \ldots, v_n), \text{ kde } a \neq 0.
\end{aligned}$$

Zřejmě β, γ a δ jsou báze. Pak

$$(\mathrm{id})_{\beta\alpha}(-,k) = \begin{cases} E_n(-,k) \text{ pro } k \neq i,j \\ E_n(-,i) \text{ pro } k = j \\ E_n(-,j) \text{ pro } k = i \end{cases}$$

$$(\mathrm{id})_{\gamma\alpha}(-,k) = \begin{cases} E_n(-,k) \text{ pro } k \neq i \\ E_n(-,i) + E_n(-,j) \text{ pro } k = i \end{cases}$$

$$(\mathrm{id})_{\delta\alpha}(-,k) = \begin{cases} E_n(-,k) \text{ pro } k \neq i \\ a \cdot E_n(-,i) \text{ pro } k = i \end{cases}$$

Povšimněte si, jak se liší β, γ a δ od α. Uvědomte si, že

$$(\mathrm{id})_{\alpha\beta} = (\mathrm{id})_{\beta\alpha}$$

$$(\mathrm{id})_{\alpha\gamma}(-,k) = \begin{cases} E_n(-,k) \text{ pro } k \neq i \\ E_n(-,i) - E_n(-,j) \text{ pro } k = i \end{cases}$$

$$(\mathrm{id})_{\alpha\delta}(-,k) = \begin{cases} E_n(-,k) \text{ pro } k \neq i \\ a^{-1} \cdot E_n(-,i) \text{ pro } k = i \end{cases}$$

Povšimněte si, že pro každou matici přechodu M se $(\mathrm{id})_{\beta\alpha} \cdot M$ liší od M tím, že je vyměněn i-tý a j-tý řádek, $M \cdot (\mathrm{id})_{\beta\alpha}$ se od M liší tím, že je vyměněn i-tý a j-tý sloupec. Podobně $(\mathrm{id})_{\gamma\alpha} \cdot M$ je shodná s M až na to, že k i-tému řádku je přičten j-tý, $(\mathrm{id})_{\delta\alpha} \cdot M$ má v i-tém řádku a-násobek i-tého řádku M, při násobení $(\mathrm{id})_{\gamma\alpha}$ a $(\mathrm{id})_{\delta\alpha}$ zprava podobně pro sloupce.

Maticím $(\mathrm{id})_{\beta\alpha}$, $(\mathrm{id})_{\gamma\alpha}$ a$(\mathrm{id})_{\delta\alpha}$ říkáme *matice elementárních úprav* nebo *elementární matice*.

Je snadné odvodit algoritmus (a především dokázat jeho konečnost), při němž budeme matici přechodu M postupně násobit zleva vhodnými elementárními maticemi tak, že nakonec dostaneme jednotkovou matici E_n, přesněji

$$E_n = U_s \cdot U_{s-1} \cdot \cdots \cdot U_1 \cdot M,$$

kde U_k označuje příslušnou elementární matici. Pak ale

$$M^{-1} = U_s \cdot U_{s-1} \cdot \cdots \cdot U_1$$

a tedy výše uvedený algoritmus je vlastně efektivním algoritmem na výpočet inverzní matice. Tento algoritmus nazýváme *Gaussův eliminační algoritmus*.

Poznámka. Uvědomte si, že podle předchozího cvičení a příkladu je

$$M = U_1^{-1} \cdot \cdots \cdot U_s^{-1},$$

tedy každá matice přechodu je součinem elementárních matic, neboť inverzní matice k elementárním maticím jsou opět elementární matice – u matic tvaru $(\mathrm{id})_{\alpha\beta}$ a $(\mathrm{id})_{\alpha\delta}$ je to zřejmé, matici $(\mathrm{id})_{\alpha\gamma}$ dostaneme vynásobením elementární matice pro přičtení j-tého k i-tému řádku maticí pro násobení j-tého řádku skalárem -1.

Cvičení. Formulujte přesně algoritmus Gaussovy eliminace a dokažte jeho konečnost.

Příklad 27. Uvažme v $\mathbb{Q}[x]_1$ bázi $\varepsilon = (1, x)$. Prozkoumáme, zda je matice

$$M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

maticí přechodu. Protože

$$(1, x) \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = (1 + 3x, 2 + 4x),$$

ověříme, zda vektory $1 + 3x$ a $2 + 4x$ jsou lineárně nezávislé. Předpokládejme, že

$$a \cdot (1 + 3x) + b \cdot (2 + 4x) = 0,$$

pak

$$a + 2b = 0$$
$$3a + 4b = 0$$

podle porovnání koeficientů u stejných mocnin. To je ale možné jedině tehdy, pokud $a = b = 0$ a tedy $1 + 3x$ a $2 + 4x$ jsou lineárně nezávislé vektory. Protože je jich stejný počet jako vektorů báze $(1, x)$, je také $\alpha = (1 + 3x, 2 + 4x)$ báze v $\mathbb{Q}[x]_1$ a tedy matice M je maticí přechodu, $M = (\mathrm{id})_{\alpha\varepsilon}$. Její inverzí je pak matice přechodu od α k ε, tedy matice složená ze sloupců souřadnic $(1)_\alpha$ a $(x)_\alpha$, které získáme z rovnic

$$1 = a \cdot (1 + 3x) + b \cdot (2 + 4x)$$
$$x = c \cdot (1 + 3x) + d \cdot (2 + 4x)$$

Dostáváme pak

$$(1)_\alpha = \begin{pmatrix} a \\ b \end{pmatrix}, (x)_\alpha = \begin{pmatrix} c \\ d \end{pmatrix}, (\mathrm{id})_{\varepsilon\alpha} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

a ověřte výpočtem, že výsledná matice přechodu je skutečně inverzní k M.

Poznámka. Promyslete si, jak jsme v předchozím příkladu dokázali, že matice M je maticí přechodu. Jádrem důkazu je to, zda jsou vektory uspořádané n-tice $\varepsilon \cdot M$ lineárně nezávislé. To je v jistém smyslu vnější kritérium, protože zkoumáme, jak se matice chová. Následující tvrzení popisuje vnitřní kritérium, zda je matice M maticí přechodu, tedy kritérium využívající jen prvků matice M.

Tvrzení. *Nechť $\alpha = (v_1, \dots, v_n)$ je báze ve V nad $\mathbb{K}$ a $M \in \mathrm{Mat}_{n\times n}(\mathbb{K})$. Pak uspořádaná n-tice vektorů $\alpha \cdot M$ je lineárně nezávislá ve V právě tehdy, když jsou sloupce matice M lineárně nezávislé jako vektory v $\mathrm{Mat}_{n\times 1}(\mathbb{K})$.*

Poznámka. Uvědomte si dobře, že lineární nezávislost sloupců M znamená, že každá lineární kombinace

$$c_1 \cdot M(-,1) + \cdots + c_n \cdot M(-,n) = 0$$

je triviální, tedy $c_1 = \cdots = c_n = 0$. Zapišme formálně skaláry $c_1, \dots, c_n$ jako n-sloupec c, tedy $c(i,1) = c_i$ pro $i = 1, \dots, n$. Protože násobení v $\mathbb{K}$ je komutativní, lze přepsat předchozí výraz jako

$$M(-,1) \cdot c(1,1) + \cdots + M(-,n) \cdot c(n,1) = M \cdot c.$$

To je mimochodem jeden z důvodů, proč jsme požadovali v definici pole komutativitu (tedy komutativitu násobení). Uvědomte si také, že jsme úplně stejnou změnu zápsiu provedli již ve výrazu 13.

Můžeme tedy říci, že sloupce matice M jsou lineárně nezávislé právě tehdy, pokud jediný n-sloupec c splňující $M \cdot c = 0$ je nulový.

Nyní dokážeme tvrzení.

Důkaz. K důkazu vyžijeme zápis lineární nezávislosti v 14. Předpokládejme, že $\alpha \cdot M$ je lineárně nezávislé. Nechť pro n-sloupec c platí $M \cdot c = 0$. Pak ale $\alpha \cdot M \cdot c = 0$ a tedy c je lineární kombinace, která nuluje $\alpha \cdot M$. Z lineární nezávislosti $\alpha \cdot M$ je potom $c = 0$ a tedy M má lineárně nezávislé sloupce.

Naopak, nechť M má lineárně nezávislé sloupce a $(\alpha \cdot M) \cdot c = 0$ pro nějaký n-sloupec c. Pak ale z lineární nezávislosti α plyne, že $M \cdot c = 0$ a z lineární nezávislosti sloupců M dostáváme $c = 0$, tedy $\alpha \cdot M$ je lineárně nezávislá. Tím je důkaz ukončen. □

Příklad 28. Povšimněme si nyní prostoru n-sloupců nad $\mathbb{K}$. Není těžké ověřit, že sloupce jednotkové matice E_n tvoří bázi tohoto prostoru, označme ji ε. Přesněji,

$$\varepsilon = \big(E_n(-,1), \dots, E_n(-,n)\big).$$

V této bázi je i-tá souřadnice vektoru c rovna prvku $c(i,1)$, tedy i-tému prvku sloupce. To může být silně matoucí, protože při nevhodném zápisu může být problém odlišit vektor souřadnic od vektoru samotného. Skutečně, $(c)_\varepsilon = c$.

Uvažme nyní n-sloupec d, který má všechny prvky $d(i,1), \dots, d(n,1)$ rovny nule. Uvědomte si, že pak $d \in \mathrm{Lin}\big(E_n(-,1), \dots, E_n(-,i-1)\big)$. Tedy matice, která má v i-tém sloupci na i-tém místě nenulový prvek a dále nuly, má lineárně nezávislé sloupce.

Připomeňme, že jsme v 26 ukázali, že Gaussův eliminační algoritmus matici přechodu postupným násobením elementárními maticemi převede na jednotkovou matici. Co se ale stane, pokud matice M není maticí přechodu a budeme ji postupně násobit

elementárními maticemi zleva? Nesouvisí to nějak s tím, jak vypadají a kolik je těch čtvercových matic, které nejsou maticemi přechodu?

Abychom dokázali odpovědět na tyto otázky, budeme muset zcela změnit pohled na matice a zavést dokonce nový druh součinu matic.

3. Lineární zobrazení, vektorové podprostory a soustavy rovnic

Příklad 29. Nechť $M \in \mathrm{Mat}_{n\times n}(\mathbb{K})$ a $v \in V$ je libovolný vektor se souřadnicemi $(v)_\alpha$ vzhledem k nějaké bázi α. Dokud jsme chápali matici M jako matici přechodu, předpokládali jsme, že existuje nějaká báze β ve V tak, že

$$(v)_\beta = M \cdot (v)_\alpha.$$

Nyní ale uvažujme jen jednu bázi a chápejme $M \cdot (v)_\alpha$ jako souřadnice nějakého jiného vektoru vzhledem k α. Tímto procesem je definováno zobrazení $V \to V$, přesněji, dostáváme zobrazení $f : V \to V$ splňující

$$f(v) = \alpha \cdot M \cdot (v)_\alpha.$$

Zdůrazněme, že je to úplně jiné použití matice než dosud – zatímco při násobení maticí přechodu se měnily zároveň souřadnice a báze a vektor zůstával stále týž, nyní se mění souřadnice a vektor, ale báze zůstává stejná.

Poznámka. Povšimněte si, že pokud má M lineárně nezávislé sloupce a $v_1, \ldots, v_k$ jsou lineárně nezávislé, pak i $f(v_1), \ldots, f(v_k)$ jsou lineárně nezávislé, specielně $f(\alpha)$ je opět báze a obrazem vektorového prostoru V v zobrazení f je opět V. Protože je násobení matice n-sloupcem distributivní podle 24, platí navíc pro každé $u, v \in V$ a každé $c \in \mathbb{K}$

$$f(u+v) = \alpha \cdot M \cdot (u+v)_\alpha = \alpha \cdot M \cdot (u)_\alpha + \alpha \cdot M \cdot (v)_\alpha = f(u) + f(v) \tag{16}$$

$$f(c \cdot u) = \alpha \cdot M \cdot (c \cdot u) = \alpha \cdot M \cdot c \cdot (u)_\alpha = c \cdot f(u).. \tag{17}$$

Definice. Nechť V a W jsou vektorové prostory nad stejným polem $\mathbb{K}$. Zobrazení $f : V \to W$ splňující vlastnosti 16–17 nazýváme *lineární zobrazení.*

Poznámka. Nemá smysl uvažovat lineární zobrazení mezi vektorovými prostory nad různými poli, protože ve vlastnosti 17 pak na obou stranách rovnosti nevystupují stejné skaláry.

Cvičení. Nechť $f : U \to V$ a $g : V \to W$ jsou lineární zobrazení. Dokažte, že pak také $g \circ f : U \to W$ je lineární zobrazení.

Cvičení. Nechť V je vektorový prostor nad $\mathbb{K}$ a $\alpha = (v_1, \ldots, v_n)$ jeho báze. Označme přiřazení souřadnic vzhledem k bázi α symbolem

$$\alpha : V \to \mathrm{Mat}_{n\times 1}(\mathbb{K}), \quad \text{kde } \alpha(v) = (v)_\alpha.$$

Dokažte, že jde o lineární zobrazení.

Nechť V a W jsou dva vektorové prostory nad stejným polem $\mathbb{K}$. Popíšeme všechna lineární zobrazení mezi těmito vektorovými prostory. Napřed ale musíme mírně zobecnit součin matic.

Definice. Nechť $M \in \mathrm{Mat}_{k\times l}(R)$ a $N \in \mathrm{Mat}_{l\times m}(R)$. Definujme součin matic M a N jako matici $P \in \mathrm{Mat}_{k\times m}(R)$ splňující

$$P(i,j) = M(i,-) \cdot N(-,j),$$

kde násobení na pravé straně označuje násobení l-řádku l-sloupcem.

Poznámka. Vidíme, že toto násobení je formálně definováno stejně jako násobení čtvercových matic v 22. Uvědomte si ale, že v žádném případě nejde o operaci nebo něco podobného. Násobení čtvercových matic je přitom speciálním případem právě definovaného násobení. Uvědomte si, že bez předpokladu stejného počtu řádků v matici M jako sloupců v matici N by nebylo možné násobení definovat.

Uvědomte si také, že násobení n-sloupce zleva maticí $n \times n$ je speciálním případem právě definovaného násobení matic, podobně násobení n-řádku maticí $n \times n$ zprava (včetně formálně poněkud odlišného násobení uspořádané báze maticí).

Příklad 30. Nechť $\alpha = (v_1, \ldots, v_n)$ je báze vektorového prostoru V nad polem $\mathbb{K}$ a $\beta = (w_1, \ldots, w_k)$ je báze vektorového prostoru W nad týmž polem $\mathbb{K}$. Mějme matici $M \in \mathrm{Mat}_{k\times n}(\mathbb{K})$. Nechť $v \in V$ je libovolný vektor. Pak

$$M \cdot (v)_\alpha$$

je k-sloupec, který můžeme ho chápat jako sloupec souřadnic nějakého vektoru ve W vzhledem k bázi β, neboli jinak řečeno, násobení maticí M zadává zobrazení $f : V \to W$ splňující

$$f(v) = \beta \cdot M \cdot (v)_\alpha.$$

Cvičení. Dokažte, že $f : V \to W$ z předchozího příkladu je lineární zobrazení, tedy zobrazení splňující 16 a 17.

Poznámka. Uvědomte si, že z jednoznačnosti souřadnic plyne, že násobení maticí M převádí souřadnice vektoru v vzhledem k bázi α na souřadnice vektoru $f(v)$ vzhledem k bázi β.

Příklad 31. Nechť $f : V \to W$ je lineární zobrazení, $\alpha = (v_1, \ldots, v_n)$ je báze ve V a β báze ve W. Definujme matici $(f)_{\beta\alpha}$ předpisem

$$(f)_{\beta\alpha}(-,i) = \big(f(v_i)\big)_\beta.$$

Pak zřejmě pro každý vektor $v \in V$ platí

$$f(v) = f\big(\alpha \cdot (v)_\alpha\big) = \alpha \cdot (f)_{\beta\alpha} \cdot (v)_\alpha$$

z definice matice $(f)_{\beta\alpha}$ a linearity f.

Definice. Matici $(f)_{\beta\alpha}$ z předchozího příkladu nazýváme *matice lineárního zobrazení $f : V \to W$ vzhledem k bazím α a β.*

Cvičení. Dokažte, že matice zobrazení je dána jednoznačně.

Příklad 32. Uvědomte si především to, že každé lineární zobrazení je úplně určeno hodnotami na bázi, přesněji, nechť $f : V \to W$ je lineární zobrazení a $\alpha = (v_1, \ldots, v_n)$ je báze ve V, pak pro každý vektor $v \in V$ je vektor $f(v) \in W$ z vlastností 16 a 17 roven

$$f(v) = f(\alpha) \cdot (v)_\alpha,$$

kde $f(\alpha)$ označuje obraz báze α. Nejde vlastně o nic jiného než v příkladu 30.

Důsledek. *Každé lineární zobrazení je plně určeno maticí zobrazení vzhledem ke zvoleným bazím, tedy lineárních zobrazení je „právě tolik jako matic“.*

Poznámka. Srovnejte si, jak je definována matice přechodu a matice zobrazení. V matici zobrazení $(f)_{\beta\alpha}$ jsou v i-tém sloupci souřadnice obrazu i-tého vektoru báze α vzhledem k bázi β. V matici přechodu $(\mathrm{id})_{\delta\gamma}$ jsou v i-tém sloupci souřadnice i-tého vektoru báze γ vzhledem k bázi δ. Podobnost není náhodná, naopak. Tuto podobnost také odráží dosud nevysvětlené značení matice přechodu. Identické zobrazení $V \to V$ zadané předpisem $\mathrm{id}(v) = v$ je jistě lineární. Jsou-li γ a δ báze v témže vektorovém prostoru V, je matice přechodu $(\mathrm{id})_{\delta\gamma}$ maticí lineárního zobrazení $\mathrm{id} : V \to V$ vzhledem k bazím γ a δ.

Poznámka. Dosud jsme se nezabývali algebraickými vlastnostmi obecného násobení matic. Protože skládání zobrazení je vždy asociativní a násobení matic představuje (lineární) zobrazení, je také násobení matic nutně asociativní. Díky tomu jsme se vlastně nemuseli zabývat výpočtem v příkladu 23.

Cvičení. Nechť $f : U \to V$ a $g : V \to W$ jsou lineární zobrazení, α báze U, β báze V a γ báze W. Dokažte, že platí

$$(g \circ f)_{\gamma\alpha} = (g)_{\gamma\beta} \cdot (f)_{\beta\alpha}.$$

Poznámka. Nyní je vhodná chvíle, abychom zdůvodnili, proč píšeme báze do řádků a souřadnice do sloupců. Už jsme vysvětlili, že nemůžeme psát obojí do řádků či sloupců, protože by pak nebylo možné definovat asociativní násobení mezi čtvercovými maticemi, takže šlo o zásadní problém. Zápis bazí do řádků a souřadnic do sloupců je jen konvence, ale jde o speciální případ velmi obecné konvence. Uvědomte si, že maticemi zobrazení násobíme n-sloupce souřadnic zleva. Kdybychom souřadnice psali do řádků, museli bychom násobit maticí zobrazení zprava. Kdybychom pak skládali dvě lineární zobrazení, např. $f : U \to V$ a $g : V \to W$, psali bychom

$$(g \circ f)_{\gamma\alpha} = (f)_{\beta\alpha} \cdot (g)_{\gamma\beta}.$$

Protože se vžilo skládání funkcí zleva, je vhodné stejným způsobem zavést i skládání, tedy násobení, matic zobrazení.

Autor textu si dovoluje podotknout, že osobně považuje skládání funkcí zleva za nevhodný přežitek a dal by přednost psaní, ke kterému už přešla část matematiků zabývajících se teorií kategorií, kteří píší napřed argument a pak postupně všechna aplikovaná zobrazení, jako např. $y = (x; \sin; \arccos)$ ve významu $y = \arccos\big(\sin(x)\big)$. V případě některých funkcí se tento zápis totiž již užívá, konkrétně píšeme $y = x^2$ a nikoli $y = {}^2(x)$.

Pokud by někdy došlo k názorovému zvratu a skutečně se začalo skládat zprava, doporučujeme změnit značení matic přechodu, tedy pro matici $f : V \to W$ vzhledem k bazím α ve V a β ve W použít symbol $(f)_{\alpha\beta}$. Při skládání pak totiž budou stejné báze vedle sebe, tedy v

$$(f; g)_{\alpha\gamma} = (f)_{\alpha\beta} \cdot (g)_{\beta\gamma}$$

jdeme na pravé straně rovnosti zobrazením f od α k β a zobrazením g od β ke γ, což je jednak estetické, jednak umožňuje kontrolu, zda pracujeme správně. Uvědomte

si, že zdánlivě obrácený zápis, který používáme pro matice zobrazení nyní, odpovídá konvenci skládání zleva.

Příklad 33. Nechť V a W jsou vektorové prostory nad týmž polem, α a β báze ve V, γ a δ báze ve W, nechť $f : V \to W$ je lineární zobrazení. Pak z předchozího cvičení plyne

$$(f)_{\delta\alpha} = (\mathrm{id})_{\delta\gamma} \cdot (f)_{\gamma\beta} \cdot (\mathrm{id})_{\beta\alpha}.$$

Toto tvrzení lze zachytit přehledným diagramem

$$\begin{array}{ccc} V_\beta & \xrightarrow{(f)_{\gamma\beta}} & W_\gamma \\ {\scriptstyle (\mathrm{id})_{\beta\alpha}}\uparrow & & \downarrow{\scriptstyle (\mathrm{id})_{\delta\gamma}} \\ V_\alpha & \xrightarrow[(f)_{\delta\alpha}]{} & W_\delta \end{array}$$

kde V_α označuje vektorový prostor V s bazí α a podobně v ostatních případech. Diagramy tohoto druhu budeme občas využívat.

Příklad 34. Nechť $f : V \to V$ je lineární zobrazení. Pak především matice f vzhledem k libovolným bazím ve V je čtvercová matice. Nechť k f existuje inverzní zobrazení $f^{-1} : V \to V$, tedy

$$f \circ f^{-1} = \mathrm{id} = f^{-1} \circ f.$$

Nechť α je libovolná báze ve V. Pak ale

$$(f \circ f^{-1})_{\alpha\alpha} = (\mathrm{id})_{\alpha\alpha} = E$$

a podobně pro $f^{-1} \circ f$. Nechť β je též báze ve V, pak podle předchozího cvičení

$$(f \circ f^{-1})_{\alpha\alpha} = (f)_{\alpha\beta} \cdot (f^{-1})_{\beta\alpha}$$

a tedy $(f^{-1})_{\beta\alpha}$ je inverzní matice k $(f)_{\alpha\beta}$. (Povšimněte si, že je to inverze oboustranná, ne jen pravá.)

Cvičení. Zajímavější je však to, že celou úvahu můžeme nyní otočit: Má-li lineární zobrazení $f : V \to V$ invertibilní matici $(f)_{\beta\alpha}$ vzhledem k nějakým bazím α a β ve V, pak je invertibilní. Dokažte, že zobrazení $g : V \to V$ zadané předpisem

$$g(v) = \alpha \cdot \Big((f)_{\beta\alpha}\Big)^{-1} \cdot (v)_\beta$$

je hledaným inverzním zobrazením.

Poznámka. Nechť je matice lineárního zobrazení $f : V \to V$ vzhledem k bazím α a β invertibilní. Pak je invertibilní matice $(f)_{\delta\gamma}$ pro libovolné báze γ a δ ve V, neboť

$$(f)_{\delta\gamma} = (\mathrm{id} \circ f \circ \mathrm{id})_{\delta\gamma} = (\mathrm{id})_{\delta\beta} \cdot (f)_{\beta\alpha} \cdot (\mathrm{id})_{\alpha\gamma}$$

a protože matice přechodu jsou invertibilní, dostáváme

$$\Big((f)_{\delta\gamma}\Big)^{-1} = (\mathrm{id})_{\gamma\alpha} \cdot \Big((f)_{\beta\alpha}\Big)^{-1} \cdot (\mathrm{id})_{\beta\delta}.$$

Cvičení. Nakreslete si schematické diagramy zachycující tvrzení předešlého příkladu a poznámky. Ujistěte se, že vše dobře chápete.

Příklad 35. Dosud jsme se nijak nepřiblížili pochopení toho, jak vypadají čtvercové matice, které jsou invertibilní. K tomu je potřeba prozkoumat některé vlastnosti lineárních zobrazení.

Především z vlastností lineárního zobrazení plyne, že nulový vektor se vždy zobrazuje na nulový vektor. To však znamená, že pokud zobrazení $f : V \to V$ zobrazuje nenulový vektor $v \in V$ na nulový vektor, nemůže mít inverzní zobrazení. Skutečně, pro každé $g : V \to V$ pak platí $(g \circ f)(v) = 0$ a tedy $(g \circ f) \neq \mathrm{id}$.

To ale znamená, že pokud jsou obrazy bázových vektorů v zobrazení $f : V \to V$ lineárně závislé, neexistuje k f inverzní zobrazení. Skutečně, nechť $\alpha = (v_1, \ldots, v_n)$ je báze ve V a $f : V \to V$ lineární zobrazení, nechť je netriviální lineární kombinace

$$c_1 \cdot f(v_1) + \cdots + c_n \cdot f(v_n) = 0.$$

Pak ale podle 16 a 17 je

$$f(c_1 \cdot v_1 + \cdots + c_n \cdot v_n) = 0$$

a protože α je lineárně nezávislé množina, znamená to, že f zobrazuje nenulový vektor $c_1 \cdot v_1 + \cdots + c_n \cdot v_n$ na nulu, tedy f nemůže mít inverzi.

Naopak, jsou-li obrazy bázových vektorů lineárně nezávislé, tvoří podle poznámky k příkladu 29 bázi $\beta = \big(f(v_1), \ldots, f(v_n)\big)$ ve V a podle 32 stačí lineární zobrazení zadat na bázi, tedy předpisem

$$g(f(v_i)) = v_i$$

dostáváme lineární zobrazení $g : V \to V$, které je zřejmě inverzní k f.

Příklad 36. Nechť $\alpha = (v_1, \ldots, v_n)$ je báze ve V a $\beta = (w_1, \ldots, w_n)$ je báze ve W. Pak $f : V \to W$ zadané na prvcích báze α předpisem $f(v_i) = w_i$ má matici

$$(f)_{\beta\alpha} = E_n.$$

K f zřejmě existuje inverzní zobrazení $f^{-1} : W \to V$ – stačí jej zadat na prvcích báze β předpisem $f^{-1}(w_i) = v_i$. Povšimněte si, že naopak každé lineární zobrazení mezi prostory stejné dimenze, které zobrazuje bázi na lineárně nezávislou množinu, je invertibilní.

Uvažme nyní vektorový prostor U s bazí $\gamma = (u_1, \ldots, u_k)$ a lineární zobrazení $g : U \to V$. Je-li $k > n$, nemůže být $g(\gamma)$ lineárně nezávislá množina, tedy existuje takový nenulový vektor $u \in U$, že

$$g(u) = g\big(\gamma \cdot (u)_\gamma\big) = \alpha \cdot (g)_{\alpha\gamma} \cdot (u)_\gamma = 0.$$

Přitom ale γ je lineárně nezávislá, tedy g zobrazuje nenulový vektor na nulový vektor a stejnou úvahou jako v 35 snadno vidíme, že ke $g : U \to V$ nemůže existovat inverzní zobrazení.

Je-li $k < n$, jistě lze definovat lineární zobrazení $g : U \to V$ tak, že $g(\gamma)$ je lineárně nezávislá, např. předpisem $g(u_i) = v_i$. Také lze snadno definovat lineární zobrazení $h : V \to U$ tak, že $h \circ g = \mathrm{id} : U \to U$, např. předpisem

$$h(v_i) = \begin{cases} u_i \text{ pro } i = 1, \ldots, k \\ 0 \text{ jinak} \end{cases}$$

To ale není inverzní zobrazení, neboť po inverzním zobrazení požadujeme také $g \circ h = \mathrm{id} : V \to V$. Protože však $n > k$, můžeme aplikovat předešlou úvahu a snadno vidíme, že takové $h : V \to U$ nemůže existovat.

To ovšem znamená, že invertibilní lineární zobrazení existují jen mezi prostory stejné dimenze, jinak řečeno, matice zobrazení může být invertibilní jen tehdy, pokud je čtvercová.

Cvičení. Vypočtěte matice zobrazení f^{-1}, g a h z předchozího příkladu, jak pro případ $k < n$, tak $k > n$, pokud je to možné.

Definice. Nechť V a W jsou vektorové prostory nad týmž polem a nechť existují lineární zobrazení $f : V \to W$ a $f^{-1} : W \to V$ tak, že $f \circ f^{-1} = \mathrm{id} : W \to W$ a $f^{-1} \circ f = \mathrm{id} : V \to V$. Pak řekneme, že prostory V a W jsou *isomorfní* a píšeme $V \simeq W$. Zobrazení f (a také f^{-1}) nazýváme *isomorfismus*.

Poznámka. Vzhledem k příkladu 36 už víme, že konečněrozměrné vektorové prostory jsou isomorfní právě tehdy, pokud mají stejnou dimenzi. Povšimněte si také, že isomorfismus je především bijektivní lineární zobrazení.

Cvičení. Nechť $\alpha = (v_1, \ldots, v_n)$ je báze ve vektorovém prostoru V nad polem $\mathbb{K}$. Dokažte, že zobrazení $\alpha : V \to \mathrm{Mat}_{n\times 1}(\mathbb{K})$ zadané předpisem $\alpha(v) = (v)_\alpha$ je isomorfismus. Uvědomte si, jak vypadá jeho inverze.

Poznámka. To tedy znamená, že každý n-rozměrný prostor je isomorfní s prostorem n-sloupců. Uvědomte si, že těchto isomorfismů je právě tolik, kolik je v prostoru bazí.

Cvičení. Nechť α je báze ve V a β báze ve W, $f : V \to W$ lineární zobrazení. Dokažte, že matice $(f)_{\beta\alpha}$ je invertibilní právě tehdy, pokud je čtvercová a má lineárně nezávislé sloupce.

Poznámka. Vidíme tedy, že matice isomorfismů mají stejné vlastnosti jako matice přechodu. To umožňuje chápat $GL(n, \mathbb{K})$ nikoli jako grupu matic přechodu, ale jako grupu matic isomorfismů prostoru $\mathrm{Mat}_{n\times 1}(\mathbb{K})$ na sebe.

Příklad 37. Nechť $f : V \to W$ je lineární zobrazení, $\alpha = (v_1, \ldots, v_n)$ je báze ve V. Z vlastností 16 a 17 plyne, že obrazem f je lineární obal obrazů vektorů báze α, přesněji

$$f(V) = \mathrm{Lin}\big(f(\alpha)\big).$$

Označení. Obraz lineárního zobrazení budeme značit $\mathrm{Im}\, f$.

Dosud jsme o lineárních obalech neřekli celou řadu podstatných věcí. Nejpodstatnější je ta, že pro libovolnou množinu vektorů $S \subseteq U$, kde U je vektorový prostor nad $\mathbb{K}$, je $\mathrm{Lin}(S) \subseteq U$ vektorový prostor. Skutečně, je-li $S = \emptyset$, je $\mathrm{Lin}(S) = \{0\}$, což je vektorový prostor. Pokud je S neprázdná, ukážeme, že pro libovolné vektory $u_1, \ldots, u_k \in \mathrm{Lin}(S)$ je libovolná lineární kombinace $c_1 \cdot u_1 + \cdots + c_k \cdot u_k$ opět prvkem $\mathrm{Lin}(S)$. Především každý u_i musí být lineární kombinací prvků S, pišme

$$u_i = d_{i1} \cdot x_{i1} + d_{i2} \cdot x_{i2} + \cdots + d_{ij_i} \cdot x_{ij_i}.$$

Pak ale

$$c_1 u_1 + \cdots + c_k u_k = c_1(d_{11}x_{11} + \cdots + d_{1j_1}x_{1j_1}) + \cdots + c_k(d_{k1}x_{k1} + \cdots + d_{kj_k}x_{kj_k}),$$

což je ale díky distributivitě opět lineární kombinace vektorů z S.

Definice. Nechť V je vektorový prostor nad polem $\mathbb{K}$ a $S \subseteq V$ neprázdná podmnožina, která je vektorovým prostorem vzhledem k operacím součtu a skalárního násobení z V. Pak S nazýváme *vektorový podprostor* ve V.

Příklad 38. V každém vektorovém prostoru V existují dva význačné podprostory – prostor V samotný a prostor $\{0\}$.

Prostor polynomů $\mathbb{Q}[x]_n$ je podprostorem v $\mathbb{Q}[x]$. Navíc pro $k \leq n$ je $\mathbb{Q}[x]_k$ podprostor v $\mathbb{Q}[x]_n$. Nejsou to ale podprostory jediné, např. prostor polynomů se sudými dimenzemi

$$\{a_n x^n + \cdots + a_1 x + a_0; a_i \in \mathbb{Q}, a_{2i+1} = 0\}$$

nebo polynomy s nulovým absolutním členem

$$\{a_n x^n + \cdots + a_1 x; a_i \in \mathbb{Q}\}$$

jsou také podprostory v $\mathbb{Q}[x]$.

V prostoru n-sloupců jsou podprostorem např. n-sloupce s nulovým i-tým prvkem

$$\{M \in \mathrm{Mat}_{n\times 1}(\mathbb{K}); M(i,1) = 0\}.$$

Nechť N je libovolný pevně zvolený n-řádek, pak

$$\{N \cdot M = 0; M \in \mathrm{Mat}_{n\times 1}(\mathbb{K})\}$$

je podprostor v prostoru n-sloupců. Uvědomte si, že prostor n-sloupců s nulovým i-tým prvkem je speciální případ pro

$$N(1,j) = \begin{cases} 1 \text{ pro } j = i \\ 0 \text{ jinak.} \end{cases}$$

Cvičení. Dokažte tvrzení předchozího příkladu.

Cvičení. Nechť V je vektorový prostor nad $\mathbb{K}$ a $U \subseteq V$ splňuje

$$\forall u, v \in U : u + v \in U \tag{18}$$

$$\forall u \in U \forall c \in \mathbb{K} : c \cdot u \in U. \tag{19}$$

Dokažte, že pak U je podprostor ve V. Uvědomte si naopak, že každý podprostor musí splňovat 18 a 19.

Cvičení. Dokažte, že průnik vektorových podprostorů je vektorový podprostor. Rozmyslete si, zda to platí jen pro průnik konečně mnoha množin, nebo pro obecný průnik.

Cvičení. Dokažte pomocí předchozího cvičení, že lineární obal množiny $S \subseteq V$ je průnikem všech vektorových podprostorů ve V, které obsahují množinu S. Uvědomte si, že z toho vyplývá, že $\mathrm{Lin}(S)$ je nejmenší vektorový podprostor ve V obsahující S.

Příklad 39. Podle Steinitzovy věty a jejích důsledků platí, že každý konečněrozměrný vektorový podprostor $U \subseteq V$ má nejvýše takovou dimenzi, jako prostor V. Nechť U má bázi $\alpha = (u_1, \ldots, u_k)$, pak lze najít vektory $v_1, \ldots, v_{n-k}$ tak, že

$$\widehat{\alpha} = (u_1, \ldots, u_k, v_1, \ldots, v_{n-k})$$

je báze ve V. (Proveďte tento důkaz jako cvičení.) Uvědomte si, že potom inkluze $i_U : U \to V$, $i_U(u) = u$ je lineární zobrazení, které má vzhledem k bazím α a $\widehat{\alpha}$ matici

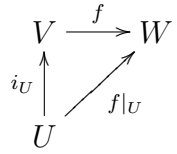
$$(i_U)_{\widehat{\alpha}\alpha} = \begin{pmatrix} E_k \\ 0_{(n-k)\times k} \end{pmatrix}, \qquad \text{přesněji } (i_U)_{\widehat{\alpha}\alpha}(i,j) = \begin{cases} 1 \text{ pro } i = j \\ \text{jinak,} \end{cases}$$

přičemž $(i_U)_{\widehat{\alpha}\alpha}$ je typu $n \times k$, kde $k \leq n$.

Zapisovat inkluzi jako zobrazení a vydělit tak podmnožinu U z V je v mnoha případech výhodnější, obzvlášť tehdy, pokud existuje další lineární zobrazení $f : V \to W$ a zajímá nás, jak se chová na podprostoru U. Pak restrikci $f|_U : U \to W$ snadno zapíšeme jako složení $f \circ i_U$ a

$$(f|_U)_{\beta\alpha} = (f)_{\beta\widehat{\alpha}} \cdot (i_U)_{\widehat{\alpha}\alpha}.$$

Symbolicky to můžeme zachytit diagramem



Cvičení. Dokažte, že obrazem vektorového podprostoru $U \subseteq V$ v lineárním zobrazení $f : V \to W$ je vektorový podprostor $f(U)$ ve W.

Označení. V dalším textu budeme používat pro nulovou matici typu $k \times n$ označení $0_{k\times n}$ jako v předchozím příkladu, pokud však budou rozměry zřejmé nebo nebudou důležité, spokojíme se s označením 0. Pozor, nepleťte si matice $0_{k\times n}$ s maticemi O_{ij} z příkladu 16. Nulové n-řádky a n-sloupce budeme i nadále značit pouze nulou, což vyžaduje jistou pozornost. Také budeme podobně jako v předchozím příkladu používat matice symbolicky sestavené z matic, tzv. blokové matice. Nebudeme je nijak pečlivě definovat a pokud nebude z kontextu zcela zřejmé, jako matici máme na mysli, pokusíme se ji zadat také přesným předpisem. Právě blokové matice jako

$$\begin{pmatrix} E \\ 0 \end{pmatrix}, \quad \begin{pmatrix} E & 0 \end{pmatrix} \text{ nebo } \begin{pmatrix} 0 & E \\ 0 & 0 \end{pmatrix}$$

budou v dalším textu velmi důležité.

Příklad 40. Motivací pro definici vektorového podprostoru pro nás bylo zjištění, že obrazem vektorového prostoru v lineárním zobrazení je lineární obal určité množiny. Nyní tedy již můžeme říci, že obrazem prosotru V v zobrazení $f : V \to W$ je podprostor $f(V) \subseteq W$.

Zajímavou otázkou je, zda každý vektorový podprostor je obrazem nějakého lineárního zobrazení. Nechť $U \subseteq V$ je vektorový podprostor, definujme zobrazení $g : V \to V$ předpisem

$$g(v) = \begin{cases} v \text{ pro } v \in U \\ 0 \text{ jinak.} \end{cases}$$

Ukažme, že toto zobrazení je lineární. Nechť $u, v \in V$, $c \in \mathbb{K}$. Pak především $u \in U$ právě tehdy, když $c \cdot u \in U$, neboť U je vektorový podprostor, tedy g splňuje 17. Je-li

$u + v \in U$, pak také

$$g(u + v) = u + v = g(u) + g(v).$$

Není-li $u + v \in U$, je více možností. Nechť $u \in U$ je nenulový vektor a $v \notin U$. Pak

$$0 = g(u + v) \neq g(u) + g(v), \text{ protože } g(u) = u \neq 0.$$

Takhle snadno to tedy nejde!

Zvolme tedy bázi α v U a doplňme ji na bázi $\widehat{\alpha}$ jako v předchozím příkladu. Definujme zobrazení $g : V \to V$ pomocí matice zobrazení. Nechť tedy

$$(g)_{\widehat{\alpha}\widehat{\alpha}}(i,j) = \begin{cases} 1 \text{ pro } i = j \leq k \\ 0 \text{ jinak,} \end{cases} \qquad \text{symbolicky } (g)_{\widehat{\alpha}\widehat{\alpha}} = \begin{pmatrix} E_k & 0_{k\times(n-k)} \\ 0_{(n-k)\times k} & 0_{(n-k)\times(n-k)} \end{pmatrix}$$

Takovému zobrazení se říká *projekce na podprostor* U a většinou se značí pr_U. Protože jde o zobrazení zadané maticí zobrazení, je lineární. Ujistěte se, že splňuje to, co splňovat má: prvních k bázových vektorů (a tedy i všechny jejich lineární kombinace) posílá na sebe, ostatní na nulu. Obrazem je tedy právě lineární obal báze α, tedy podprostor U.

Ukázali jsme tedy, že každý vektorový podprostor je obrazem vektorového prostoru ve vhodném lineárním zobrazení.

Příklad 41. Existuje ale také jiný pohled na vektorové podprostory. Nechť V a W jsou vektorové prostory a $f : V \to W$ lineární zobrazení. Nechť U je vektorový podprostor, nyní ale v prostoru W.

Vzorem U rozumíme množinu $f^{-1}(U) = \{v \in V; f(v) \in U\}$. Tato množina je vektorový podprostor ve V, neboť pro $u, v \in f^{-1}(U)$ a $c, d \in \mathbb{K}$ je $f(u), f(v) \in U$ a tedy

$$f(c \cdot u + d \cdot v) = c \cdot f(u) + d \cdot f(v) \in U$$

díky linearitě f a tomu, že U je podprostor ve W, tedy $c \cdot u + d \cdot v \in f^{-1}(U)$ a $f^{-1}(U)$ je podprostor ve V.

Uvažme obzvlášť podprostor $\{0\} \subseteq W$. Jeho vzor nazýváme *jádro* lineárního zobrazení $f : V \to W$ a značíme $\ker f$.

Poznamenejme, že jádrem zobrazení $h : S_1 \to S_2$ mezi množinami se rozumí relace ekvivalence $\equiv$ na S_1 definovaná $s \equiv r \Leftrightarrow h(s) = h(r)$. Právě definované jádro lineárního zobrazení ale není relací ekvivalence, nýbrž množinou. Pomocí jádra ale lze definovat relaci ekvivalence J_f takto:

$$J_f(v_1, v_2) \Longleftrightarrow v_1 - v_2 \in \ker f.$$

Relace J_f je pak jádrem ve smyslu relace ekvivalence. Povšimněte si, že $\ker f$ je třídou rozkladu V podle J_f, v níž je obsažen nulový vektor.

Podobně jako v předchozím příkladu můžeme ukázat, že každý vektorový podprostor je jádrem vhodného lineárního zobrazení. Nechť U je podprostor ve V. Označme

$$v + U = \{v + u; u \in U\}$$

a definujme relaci

$$v_1 + U \sim v_2 + U \text{ právě tehdy, když } v_1 - v_2 \in U.$$

Nyní položme

$$V/U = \{v + U; v \in V\}/\sim$$

a definujme operace

$$+ : V/U \times V/U \to V/U \text{ předpisem} \quad (v_1 + U) + (v_2 + U) = (v_1 + v_2) + U$$
$$\cdot : \mathbb{K} \times V/U \to V/U \text{ předpisem} \quad c \cdot (v + U) = (c \cdot v) + U$$

Cvičení. Dokažte, že $\sim$ je relace ekvivalence a že množina V/U s operacemi definovanými výše tvoří vektorový prostor nad polem $\mathbb{K}$.

Definice. Vektorovému prostoru V/U říkáme *faktorový vektorový prostor*.

Cvičení. Nyní definujme zobrazení $g : V \to V/U$ předpisem $g(v) = v + U$. Dokažte, že toto zobrazení je lineární a že $\ker g = U$.

Dokázali jsme, že každý vektorový podprostor je jádrem vhodného lineárního zobrazení.

Poznámka. Povšimněte si, že specielně $V/V \simeq \{0\}$ a $V/\{0\} \simeq V$.

Cvičení. Nechť $\alpha = (u_1, \ldots, u_k)$ je báze $U \subseteq V$ a $\widehat{\alpha} = (u_1, \ldots, u_k, v_1, \ldots, v_{n-k})$ je báze V. Dokažte, že pak $(v_1 + U, \ldots, v_{n-k} + U)$ je báze V/U.

Příklad 42. Nechť α je báze V a β báze ve W a $f : V \to W$ lineární zobrazení. Pak

$$\ker f = \{v \in V; (f)_{\beta\alpha}(v)_\alpha = 0\}.$$

Výraz

$$(f)_{\beta\alpha}(v)_\alpha = 0$$

představuje *soustavu lineárních rovnic* a vektory v, které této soustavě vyhovují, se nazývají *řešení soustavy*. Formálně můžeme sestavit soustavu lineárních rovnic pomocí *matice soustavy* $A \in \mathrm{Mat}_{k\times n}(\mathbb{K})$ a n-sloupce *neznámých* $x \in \mathrm{Mat}_{n\times 1}(\mathbb{K})$ jako výraz

$$A \cdot x = 0.$$

Nebudeme uvažovat soustavy nad obecným okruhem skalárů a nebude nás ani zajímat řešitelnost takových soustav.

Množina všech neznámých tvoří vektorový podprostor v $\mathrm{Mat}_{n\times 1}(\mathbb{K})$, neboť pro libovolná řešení x_1 a x_2 a skaláry c_1, c_2 platí

$$A \cdot (c_1 \cdot x_1 + c_2 \cdot x_2) = c_1 \cdot A \cdot x_1 + c_2 \cdot A \cdot x_2 = 0$$

díky distributivitě násobení matic.

Příklad 43. Nechť U je podprostor ve V a α báze ve V. Pak souřadnice vektorů z U tvoří řešení vhodné soustavy lineárních rovnic, tedy podprostor v $\mathrm{Mat}_{n\times 1}(\mathbb{K})$. Ukázali jsme totiž, že každý vektorový podprostor je jádrem vhodného lineárního zobrazení. Matice tohoto zobrazení je pak maticí příslušné soustavy lineárních rovnic.

Zvolme bázi α ve V tak, že prvních k vektorů generuje U. Uvědomte si, že pak maticí zobrazení $p : V \to V/U$ je matice $\big(0_{n\times(n-k)}|E_k\big)$.

Z této matice je dobře vidět, že dimenze V/U je rovna $\dim V - \dim U$, což už ale víme.

Platí ale obecnější tvrzení. Nechť $f : V \to W$ je lineární zobrazení, pak

$$\dim V = \dim \ker f + \dim \operatorname{Im} f.$$

Nejjednodušší metodou důkazu je zvolit ve V bázi $\alpha = (v_1, \ldots, v_n)$ takovou, že $\ker f = \operatorname{Lin}(v_1, \ldots, v_k)$. Uvědomte si, že $f(v_{k+1}), \ldots, f(v_n)$ jsou lineárně nezávislé vektory, neboť kdyby nějaká jejich lineární kombinace byla nulová, patřila by do $\ker f$. Tím je důkaz ukončen.

Zvolme ve W bázi $\beta = \big(f(v_{k+1}, \ldots, f(v_n), w_1, \ldots, w_l\big)$. Pak je

$$(f)_{\beta\alpha}(i,j) = \begin{cases} 1 \text{ pro } i = j > k \\ 0 \text{ jinak,} \end{cases} \qquad \text{neformálně tedy } (f)_{\beta\alpha} = \begin{pmatrix} 0 & E \\ 0 & 0 \end{pmatrix},$$

což připomíná situaci $p : V \to V/U$. Je-li f surjektivní, spodní řádek nul v $(f)_{\beta\alpha}$ zmizí. Tak je tomu právě v případě $p : V \to V/U$.

Uvědomte si, že je-li jádro triviální, zmizí sloupec nul vlevo. Povšimněte si, že jádro je triviální právě tehdy, je-li zobrazení f prosté, neboť

$$f(u) = f(v) \text{ implikuje } 0 = f(u) - f(v) = f(u - v) \text{ a tedy } u - v \in \ker f.$$

Potřebujeme-li tedy ověřit, zda je lineární zobrazení prosté, stačí ukázat, že vzorem nulového vektoru je pouze nulový vektor.

Příklad 44. Nechť $f : V \to W$ je lineární zobrazení a zvolme takové báze, že

$$(f)_{\beta\alpha} = \begin{pmatrix} 0 & E \\ 0 & 0 \end{pmatrix}.$$

Nyní definujme zobrazení $f' : V \to \operatorname{Im} f$ předpisem $f'(v) = f(v)$, tedy f' splývá s f, ale jeho obor hodnot je jen $\operatorname{Im} f$. Tedy f' je surjektivní a jeho matice

$$(f)_{\widetilde{\beta}\alpha} = \begin{pmatrix} 0 & E \end{pmatrix},$$

kde báze $\widetilde{\beta}$ je vytvořena z báze β tak, že vynecháme vektory negenerující $\operatorname{Im} f$.

Připomeňme, že inkluze $\ker f$ do V je lineární zobrazení. Zvolme v $\ker f$ bázi $\widetilde{\alpha}$, kterou vytvoříme z α vypuštěním vektorů, které negenerují $\ker f$. Pak

$$(i_{\ker f})_{\alpha\widetilde{\alpha}} = \begin{pmatrix} E \\ 0 \end{pmatrix}$$

a povšimněte si, že

$$(f \circ i_{\ker f})_{\widetilde{\beta}\widetilde{\alpha}} = \begin{pmatrix} 0 & E \end{pmatrix} \cdot \begin{pmatrix} E \\ 0 \end{pmatrix}$$

je nulová matice. Situaci lze zachytit diagramem

$$\begin{array}{ccccc} V & \xrightarrow{f} & \operatorname{Im} f & \xrightarrow{i_{\operatorname{Im} f}} & W \\ {\scriptstyle i_{\ker f}}\uparrow & \nearrow_{0} & & & \\ \ker f & & & & \end{array}$$

Cvičení. Určete rozměry všech matic v minulém příkladu, nahraďte symboly E a 0 přesnými označeními E_k a $0_{m\times n}$. Uvědomte si také, jaké rozměry má matice inkluze $i_{\operatorname{Im} f} : \operatorname{Im} f \to W$.

Příklad 45. Vraťme se k soustavám lineárních rovnic. V příkladu 38 jsme viděli, že množina

$$Z = \{N \cdot M = 0; M \in \mathrm{Mat}_{n\times 1}(\mathbb{K})\}$$

je podprostorem v prostoru n-sloupců. Výraz $N \cdot M = 0$ představuje ovšem soustavu lineárních rovnic, která je složena z jediné rovnice. Dimenze řešení této soustavy je rovna $n-1$. To proto, že N je vlastně maticí surjektivního lineárního zobrazení $f : \mathrm{Mat}_{n\times 1}(\mathbb{K}) \to \mathbb{K}$ zadaného předpisem $f(M) = N \cdot M$, množina řešení soustavy je jádrem tohoto zobrazení a dimenze $\mathbb{K}$ je rovna jedné. Podle vztahu $\dim V = \dim \ker f + \dim \mathrm{Im}\, f$ dostáváme, že $\dim Z = n-1$.

Ve skutečnosti jsme se v předchozím odstavci dopustili hrubé chyby. Pokud by N byl nulový řádek, není f surjektivní a $\dim \mathrm{Im}\, f = 0$, tedy $\dim Z = n$. To souhlasí s tím, že každý n-sloupec M je řešením soustavy $0 \cdot M = 0$.

Definice. Vektorový podprostor $U \subseteq V$, jehož dimenze je rovna $\dim V - 1$, nazýváme *nadrovina*.

Příklad 46. Nechť U a W jsou nadroviny ve V, $\dim V = n$. Uvažme průnik $U \cap W$. To je vektorový podprostor ve V. Ukážeme, že jeho dimenze je buď $n-1$ nebo $n-2$. Víme, že U je jádrem $p : V \to V/U$. Pokud je $p(W) = \{0\}$, je W podprostor v U. Protože však U a V mají stejné dimenze, je $U = W$ a $\dim U \cap V = n-1$.

Označme α bázi v U a β bázi ve W. Pokud $p(W) \neq \{0\}$, znamená to, že ve W existuje vektor w, který není prvkem U. Podle Steinitzovy věty je $\mathrm{Lin}(\alpha \cup \{w\}) = V$, takže každý další $w' \in W$ splňující $p(w') \neq 0$ je lineárně závislý na w. Nyní opět podle Steinitzovy věty lze nahradit některý vektor báze β vektorem w. Nechť výsledná báze je $(w, v_1, \ldots, v_{n-2})$ a označme $\gamma = (v_1, \ldots, v_{n-2})$. Uvědomte si, že $p\big(\mathrm{Lin}(\gamma)\big) = \{0\}$, tedy $\mathrm{Lin}(\gamma)$ je podprostor U. Protože $w \notin U$, je $\mathrm{Lin}(\gamma) = U \cap W$ a $\dim U \cap W = n-2$, neboť γ je lineárně nezávislá množina.

Příklad 47. Nechť nyní $A \cdot x = 0$ je soustava rovnic. Každý řádek této rovnice lze chápat jako n-řádek, tedy řešením soustavy je průnik nadrovin, které jsou řešeními jednotlivých rovnic. Jakou dimenzi toto řešení má? Je-li matice A typu $k \times n$, může být dimenze řešení $n-k$ až n. (V případě, že $k > n$, samozřejmě nemůže být dimenze řešení záporná.)

Skutečně, protože prostor řešení soustavy je jádrem zobrazení

$$f : \mathrm{Mat}_{n\times 1}(\mathbb{K}) \to \mathrm{Mat}_{k\times 1}(\mathbb{K}), \qquad f(M) = A \cdot M,$$

je dimenze řešení rovna rozdílu $n - \dim \mathrm{Im}\, f$. Dimenze obrazu f je rovna počtu lineárně nezávislých sloupců v matici A. Dimenzi řešení však lze vyjádřit i pomocí počtu lineárně nezávislých řádků, jak nyní ukážeme.

Příklad 48. Nechť N_1 a N_2 jsou dva n-řádky. Označme

$$U_1 = \{N_1 \cdot x = 0; M \in \mathrm{Mat}_{n\times 1}(\mathbb{K})\}, \quad U_2 = \{N_2 \cdot x = 0; M \in \mathrm{Mat}_{n\times 1}(\mathbb{K})\}$$

a průnik $U = U_1 \cap U_2$. Potom U je množina řešení soustavy rovnic zadané oběma řádky N_1 a N_2.

Podle předchozího příkladu může U mít dimenzi n, $n-1$ nebo $n-2$. První případ znamená, že oba řádky jsou nulové.

Nechť tedy $\dim U = n-2$. Nechť $M_1 \in U_1 - U$ a $M_2 \in U_2 - U$ jsou libovolné nenulové n-sloupce. Předpokládejme, že N_1 a N_2 jsou lineárně závislé, tedy existují skaláry $a, b \in \mathbb{K}$ tak, že

$$a \cdot N_1 + b \cdot N_2 = 0.$$

Protože však $N_1 \cdot M_2 \neq 0$ a $N_2 \cdot M_1 \neq 0$, musí být $a = 0 = b$.

Dimenze U je rovna $n-1$ buď tehdy, pokud je prostor řešení jedné rovnice nadrovina a druhý celý prostor n-sloupců, nebo pokud jsou U_1 a U_2 stejné nadroviny. Ukážeme, že v obou těchto případech jsou pak N_1 a N_2 lineárně závislé. Je-li jedno z řešení celý prostor, je příslušný n-řádek nulový a N_1 a N_2 jsou jistě lineárně závislé. Pokud $U_1 = U_2$, zvolme n-sloupec M, který není prvkem U. Označme $a = N_1 \cdot M$, $b = N_2 \cdot M$. Zvolme libovolný n-sloupec P. Pak

$$b \cdot N_1 \cdot P - a \cdot N_2 \cdot P = 0.$$

Pro $P \in U$ je tato rovnost splněna triviálně. Je-li $P \in \mathrm{Mat}_{n\times 1}(\mathbb{K}) - U$, je pak nenulovým násobkem n-sloupce M. Kdyby totiž P bylo lineárně nezávislé na M, nemohlo by mít U dimenzi $n-1$. Tedy

$$(b \cdot N_1 - a \cdot N_2) \cdot P = b \cdot N_1 \cdot c \cdot M - a \cdot N_2 \cdot c \cdot M = b \cdot c \cdot a - a \cdot c \cdot b = 0.$$

Protože P byl zvolen libovolně, musí být $b \cdot N_1 - a \cdot N_2$ nulový n-řádek. Protože a a b jsou nenulové, jsou N_1 a N_2 lineárně závislé.

Dostáváme tedy, že dimenze průniku dvou nadrovin zadaných rovnicemi $N_1 \cdot x = 0$ a $N_2 \cdot x = 0$ je rovna $n - \dim \mathrm{Lin}(\{N_1, N_2\})$.

Cvičení. Zobecněte předchozí příklad na soustavu m rovnic o n neznámých, tedy přesněji, dokažte, že má-li prostor řešení soustavy rovnic dimenzi k, má soustava $n-k$ lineárně nezávislých řádků.

Cvičení. Dokažte, že jsou-li N_1 a N_2 nenulové lineárně závislé n-řádky, jsou nadroviny $\{N_1 \cdot x = 0; x \in \mathrm{Mat}_{n\times 1}(\mathbb{K})\}$ a $\{N_2 \cdot x = 0; x \in \mathrm{Mat}_{n\times 1}(\mathbb{K})\}$ stejné.

Příklad 49. Jsou-li N_1 a N_2 lineárně nezávislé n-řádky, pak jsou především nenulové a tedy řešení soustav $N_1 \cdot x = 0$ a $N_2 \cdot x = 0$ jsou nadroviny. Nechť A je matice sestavená z N_1 a N_2, tedy $A(-,1) = N_1$ a $A(-,2) = N_2$. Podle 46 má prostor řešení soustavy $A \cdot x = 0$ dimenzi $n-1$ nebo $n-2$.

Nyní využijeme následující trik. Uvědomme si, že každý n-sloupec M zadává zobrazení $f : \mathrm{Mat}_{1\times n}(\mathbb{K}) \to \mathbb{K}$ předpisem $f(N) = N \cdot M$. Zvolme libovolnou bázi prostoru řešení soustavy. Ze sloupců báze sestavme matici B. Nyní zřejmě n-řádky N_1 a N_2 patří do prostoru řešení soustavy $y \cdot B = 0$. Protože jsou N_1 a N_2 lineárně nezávislé a tedy prostor řešení soustavy má dimenzi nejméně 2, může mít podle předchozích příkladů a cvičení B nejvýše $n-2$ nezávislých sloupců (díky tomu, že je celá soustava „otočená“, musíme namísto řádků v matici B pracovat se sloupci). Ale jako sloupce matice B jsme použili n-sloupce báze prostoru řešení soustavy $A \cdot x = 0$, tedy dimenze prostoru řešení je $n-2$.

Cvičení. Zobecněte předchozí příklad, tedy přesněji, dokažte, že má-li matice soustavy $A \cdot x = 0$ k lineárně nezávislých řádků, je dimenze prostoru řešení rovna $n-k$.

Poznámka. Uvědomte si, co jsme vlastně dokázali. Nechť $A \cdot x = 0$ je soustava lineárních rovnic, A typu $m \times n$. Předchozí série příkladů a cvičení ukázala, že dimenze prostoru řešení je rovna $n - k$, kde k je počet lineárně nezávislých řádků matice A.

Již ale víme, že matici A lze chápat jako matici zobrazení z n-rozměrného do m-rozměrného prostoru, přičemž dimenze obrazu tohoto zobrazení je rovna počtu lineárně nezávislých sloupců, řekněme l. Pak ale dimenze jádra je rovna $n - l$ podle 43. Ovšem jádro zobrazení zadaného maticí A je právě podprostor řešení soustavy $A \cdot x = 0$. Z toho plyne, že $k = l$, tedy počet lineárně nezávislých sloupců je roven počtu lineárně nezávislých řádků.

Definice. Počet lineárně nezávislých sloupců (a tedy i řádků) matice A nazveme *hodnost matice* a značíme $h(A)$.

Cvičení. Dokažte, že pro A typu $n \times k$ a B typu $k \times m$ je

$$h(A \cdot B) \leq \min\big\{h(A), h(B)\big\}.$$

Návod: Chápejte matice jako matice zobrazení a všímejte si dimenzí obrazů.

Poznámka. Povšimněte si, jak složité a zdlouhavé bylo ukázat, že je lineárně nezávislých sloupců v matici stejně jako lineárně nezávislých řádků. Celý důkaz vlastně začíná již příkladem 46.

Složitost důkazu není náhodná. Použili jsme totiž naprosto přímočarou metodu, která nebyla v žádném případě nejefektivnější. Zato je však v každé části použita jedna takřka ukázková metoda, jak podobná tvrzení dokazovat. V dalším textu důkaz provedeme znovu a uvidíme, že je vlastně velmi jednoduchý.

Budeme potřebovat dva jednoduché fakty o isomorfismech.

Příklad 50. Nechť $f : U \to V$ je lineární zobrazení a $g : V \to W$ isomorfismus. Protože isomorfismus je bijekce, je také prostý, tedy $\ker g = \{0\}$ podle 43. Opět podle příkladu 43 je pak dimenze $g(\operatorname{Im} f)$ rovna dimenzi $\operatorname{Im} f$.

Povšimněte si, že stejným způsobem lze ukázat, že dimenze podprostoru se isomorfismem nemění.

Specielně to znamená, že má-li čtvercová matice A typu $n \times n$ lineárně nezávislé sloupce (tj. je maticí nějakého isomorfismu), pro každou matici B typu $n \times k$ má $A \cdot B$ stejný počet lineárně nezávislých sloupců jako B.

Příklad 51. Nechť A je matice $m \times n$ a nechť B je matice isomorfismu, tedy má lineárně nezávislé sloupce. Nechť A má $k < m$ lineárně nezávislých řádků. Uvažme lineární kombinaci, která nuluje řádky A, tedy m-řádek c splňující $c \cdot A = 0$. Pak ale $c \cdot A \cdot B = 0$. Protože i-tý řádek matice $A \cdot B$ je $A(i, -) \cdot B$, je $c \cdot A \cdot B$ lineární kombinace řádků $A \cdot B$. Tedy řádky $A \cdot B$ jsou lineárně závislé.

Vyberme nyní všech k lineárně nezávislých řádků A a vytvořme z nich matici C typu $k \times n$. Ukážeme, že také $C \cdot B$ má k lineárně nezávislých řádků.

Budeme postupovat sporem, předpokládejme, že existuje nenulový k-řádek d splňující $d \cdot C \cdot B = 0$. Nechť s je libovolný nenulový n-sloupec, pak

$$d \cdot C \cdot B \cdot s = 0 \cdot s = 0.$$

Ale řádky matice C jsou lineárně nezávislé, tedy řádek $d \cdot C$ musí být nenulový. Sloupce matice B jsou lineárně nezávislé, takže sloupec $B \cdot s$ musí být nenulový. (Povšimněte si, že s představuje lineární kombinaci sloupců B.) Přitom sloupce matice B tvoří bázi v prostoru n-sloupců a protože je s zvolen libovolně, znamená to, že n-řádek $d \cdot C$ je po vynásobení libovolným n-sloupcem roven nule. To ale může platit jen pro nulový n-řádek a to je spor.

Uvědomte si, že jsme ukázali, že matice $A \cdot B$ má k lineárně nezávislých řádků.

Příklad 52. Nechť A je matice $m \times n$. Pak ji lze chápat jako matici nějakého zobrazení $f : V \to W$ vzhledem k vhodným bazím α ve V a β ve W. Nechť $\gamma = (v_1, \ldots, v_n)$ je taková báze V, že $\ker f = \operatorname{Lin}\big(\{v_1, \ldots, v_k\}\big)$. Již víme, že lze najít bázi ve W tvaru $\delta = \big(f(v_{k+1}), \ldots, f(v_n), w_1, \ldots, w_{m-n+k}\big)$. Pak zřejmě

$$(f)_{\delta\gamma} = \begin{pmatrix} 0_{(n-k)\times k} & E_{n-k} \\ 0_{(m-n+k)\times k} & 0_{(m-n+k)\times(n-k)} \end{pmatrix}.$$

Již z 28 víme, že sloupce matice E_n jsou lineárně nezávislé. Podobně v matici $(f)_{\delta\gamma}$ je posledních $(n-k)$ sloupců lineárně nezávislých. Je však také zřejmé, že právě $(n-k)$ prvních řádků je lineárně nezávislých.

Protože změny báze jsou realizovány isomorfismy $\mathrm{id} : V \to V$ a $\mathrm{id} : W \to W$ (reprezentovanými maticemi přechodu $(\mathrm{id})_{\alpha\gamma}$ a $(\mathrm{id})_{\delta\beta}$), je počet lineárně nezávislých řádků a sloupců stejný i v matici $(f)_{\beta\alpha} = A$ podle 50 a 51.

Poznámka. Uvědomte si, že kromě 51 jsme vlastně jen opakovali obecné úvahy o lineárních zobrazeních. Na rozdíl od předchozího přístupu, kdy jsme rovnost počtu lineárně nezávislých řádků a sloupců dokázali pomocí vlastností prostorů řešení příslušných soustav, vyšli jsme zde přímo z vlastností matic.

Příklad 53. Vzhledem k příkladu 26 víme, že matice přechodu jsou součiny elementárních matic. Převedení obecné matice A na tvar

$$\begin{pmatrix} 0 & E \\ 0 & 0 \end{pmatrix}$$

je tedy realizováno vynásobením vhodnými elementárními maticemi zprava a zleva. Násobení elementárními maticemi zleva provádí záměny řádků, přičtení k jinému řádku a vynásobení řádku skalárem. Násobení zprava provádí totéž se sloupci. Chápeme-li však matici A jako matici soustavy a nikoli matici lineárního zobrazení, nejsou elementární operace se sloupci příliš vhodné. Uvažme soustavu $A \cdot x = 0$ a proveďme na A nějakou elementární sloupcovou operaci, která nechť je realizována maticí U. Pak ale dostáváme soustavu $A \cdot U \cdot x = 0$. Nechť M je nějaké řešení této soustavy. Ihned vidíme, že M nemusí být řešením $A \cdot x = 0$, nechť např.

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}, \qquad U = \begin{pmatrix} -2 & 0 \\ 0 & 1 \end{pmatrix}, \qquad M = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Pak

$$A \cdot U \cdot M = \begin{pmatrix} -2 & 2 \\ -4 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \text{ ale } \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 6 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Uvědomte si, že toto není problém v případě řádkových úprav. Nechť B je libovolná elementární matice nebo obecněji libovolná matice s lineárně nezávislými sloupci. Pak podprostory řešení soustav $B \cdot A \cdot x = 0$ a $A \cdot x = 0$ jsou stejné. Skutečně, je-li M řešení $A \cdot x = 0$, pak $B \cdot A \cdot M = B \cdot 0 = 0$. Naopak nechť M je řešení $B \cdot A \cdot x = 0$. Protože má B lineárně nezávislé sloupce a sloupec $A \cdot M$ je lineární kombinace, která sloupce B nuluje, je nutně $A \cdot M = 0$. To ale znamená, že M je řešení $A \cdot x = 0$.

Poznámka. Shrňme výsledky této kapitoly. Matice mohou reprezentovat lineární zobrazení a také zadávat soustavy lineárních rovnic. Jádra a obrazy lineárních zobrazení tvoří vektorové podprostory, řešení soustav lineárních rovnic také tvoří vektorové podprostory. Matice zobrazení přitom zadává soustavu, jejíž řešení je jádrem tohoto zobrazení.

Matice má stejný počet lineárně nezávislých řádků jako sloupců. Isomorfismy mají matice zobrazení $n \times n$ s hodností n, pokud takovou matici chápeme jako matici soustavy, má jen triviální řešení. Právě čtvercové matice $n \times n$ s hodností n jsou invertibilní.

Reference

[H] Hefferon, J., Linear Algebra, kniha dostupná na webové stránce autora
`http://joshua.smcvt.edu/pub/hefferon/book/book.pdf`

[S] Slovák, J., Lineární algebra, skripta dostupná na webové stránce autora
`http://www.math.muni.cz/~slovak`

Pokud má někdo zájem, doporučuji připsat následující věci:

- Horní trojúhelníkové matice, diagonální matice a další grupy matic.
- Matice soustav ve schodovém a redukovaném schodovém tvaru.
- Transpozice matic.
- Kroneckerův (tenzorový) součin matic.
- Součty vektorových podprostorů, především vysvětlit, jak se vypočte ze soustav zadávajících jednotlivé podprostory soustava zadávající součet.

Možná by též stálo za úvahu sestavit sbírku cvičení, sestavenou ze zhovadilých příkladů.