Letmý úvod k algebraickým strukturám

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. 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:

$$\forall a, b, c \in \mathbb{Z} : a + (b + c) = (a + b) + c \qquad \text{(asociativita)} \tag{1}$$
$$\exists 0 \in \mathbb{Z} \forall a \in \mathbb{Z} : 0 + a = a + 0 = a \qquad \text{(existence neutrálního prvku)} \tag{2}$$
$$\forall a \in \mathbb{Z} \exists b \in \mathbb{Z} : a + b = 0 \qquad \text{(existence inverzního prvku)} \tag{3}$$
$$\forall a, b \in \mathbb{Z} : a + b = b + a \qquad \text{(komutativita)} \tag{4}$$

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

(6) $\quad \forall a, b, c \in \mathbb{Z} : (a + b) \cdot c = a \cdot c + b \cdot c \quad$ (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 $\big(\operatorname{Mat}_{k\times l}(\mathbb{N}),+,*\big)$ okruhem není, ale $\big(\operatorname{Mat}_{k\times l}(\mathbb{Z}),+,*\big)$ a $\big(\operatorname{Mat}_{k\times l}(\mathbb{Q}),+,*\big)$ 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

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

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 $\big(\operatorname{Mat}_{k\times l}(\mathbb{Q}),+,*\big)$. 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

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

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

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:

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

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

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 $\{v_1, \dots, v_k\} \subseteq S$ a každou množinu skalárů $\{a_1, \dots, a_k\}$ 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 $\mathbb{Z}_6 = \{0, 1, \dots, 5\}$ 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

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

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 $V = \mathrm{Lin}(\{v_1, \dots, v_k\})$. 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 $V = \mathrm{Lin}(\{v_2, \dots, v_k\})$ 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 $\{1, x, x^2, \dots, x^n, \dots\}$ je bazí v $\mathbb{Q}[x]$, podobně $\{1, x, \dots, x^n\}$ 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 $\big\{O_{i,j};\ i = 1, \dots, k,\ j = 1, \dots, l\big\}$ 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. $\alpha = (1, x, x^2, \dots, x^n)$ a $\beta = (1, 1 + x, 1 + x + x^2, \dots, 1 + x + \cdots + x^n)$ 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 $\gamma = (1 + x, x + x^2, x^2 + x^3, \dots, x^{n-1} + x^n)$. 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* $\alpha = (v_1, \dots, v_n)$ *je báze* V *nad* $\mathbb{K}$ *a* $u \neq 0$ *libovolný vektor. Pak existuje* $i = 1, \dots, n$ *takové, že* $(u, v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n)$ *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 $\{u, v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n\}$, tedy $\{u, v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n\}$ generuje V.

Kdyby nyní byla $\{u, v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n\}$ 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 $(u, v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n)$ je báze V. $\square$

Věta (Steinitz). *Nechť* $\alpha = (v_1, \dots, v_n)$ *je báze* V *nad* $\mathbb{K}$ *a* $\{u_1, \dots, u_k\}$ *je lineárně nezávislá množina vektorů. Pak* $k \leq n$ *a mezi vektory báze existuje taková* $(n-k)$*-tice* $v_{i_1}, \dots, v_{i_{n-k}}$*, že* $(u_1, \dots, u_k, v_{i_1}, \dots, v_{i_{n-k}})$ *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 $(u_1, \dots, u_{k-1}, v_{i_1}, \dots, v_{i_{n-k+1}})$ 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 $\{u_1, \dots, u_k\}$ 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 $(u_1, \dots, u_n)$, musela by být množina $\{u_1, \dots, u_k\}$ lineárně závislá. $\square$

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 $\alpha = (v_1, \ldots, v_n)$ 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

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

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 $i = 1, \dots, n$ 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

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

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:

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

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

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

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

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

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 $i = 1, \dots, n$

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

Pak lze výraz 15 přepsat jako

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\begin{aligned} A \cdot (B + C) &= A \cdot B + A \cdot C \\ (A + B) \cdot C &= A \cdot C + B \cdot C. \end{aligned}$$

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.

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

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 $\alpha = (v_1, \dots, v_n)$ báze V. Označme
$$\begin{aligned}
\beta &= (v_1, \dots, v_{i-1}, v_j, v_{i+1}, \dots, v_{j-1}, v_i, v_{j+1}, \dots, v_n),\\
\gamma &= (v_1, \dots, v_{i-1}, v_i + v_j, v_{i+1}, \dots, v_n),\\
\delta &= (v_1, \dots, v_{i-1}, a \cdot v_i, v_{i+1}, \dots, v_n), \text{ kde } a \neq 0.
\end{aligned}$$
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
$$E_n = U_s \cdot U_{s-1} \cdot \dots \cdot U_1 \cdot M,$$
kde U_k označuje příslušnou elementární matici. Pak ale
$$M^{-1} = U_s \cdot U_{s-1} \cdot \dots \cdot U_1$$
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

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

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 $a+2b = 0$ a $3a+4b = 0$ porovnáním 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

$$\begin{aligned} 1 &= a \cdot (1 + 3x) + b \cdot (2 + 4x) \\ x &= c \cdot (1 + 3x) + d \cdot (2 + 4x) \end{aligned}$$

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

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

je triviální, tedy $c_1 = \cdots = c_n = 0$. Zapišme formálně skaláry $c_1, \ldots, c_n$ jako n-sloupec c, tedy $c(i,1) = c_i$ pro $i = 1, \ldots, n$. 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. $\square$

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,

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

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

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`