Lineární algebra

Studijní text

Daniel Dombek[1], Tomáš Kalvoda[2], Luděk Kleprlík[3], Karel Klouda[4]

daniel.dombek@fit.cvut.cz tomas.kalvoda@fit.cvut.cz
ludek.kleprlik@fit.cvut.cz karel.klouda@fit.cvut.cz

KAM FIT ČVUT v Praze

LS 2017/2018

[1]Převážně kapitoly 2, 3 a 5.
[2]Převážně kapitoly 6 a 7.
[3]Všeobecné zlepšování a korektury
[4]Převážně kapitoly 1 a 4.

Obsah

Úvod (provizorní)

Milé studentky, milí studenti,

od akademického roku 2014/2015 se významně mění kurz lineární algebry. Jednou z hlavních změn je, že namísto podrobných slajdů a handoutů bude hlavním studijním materiálem tento studijní text. Jelikož text bude vznikat průběžně během semestru, bude se neustále měnit a opravovat. Doufáme, že se nám podaří, aby Vám mohl sloužit při průběžné přípravě na přednášky, na zápočtové písemky a zejména na zkoušky.

Budeme velmi rádi, když nás budete upozorňovat na chyby, překlepy či na nesrozumitelné části textu. Jak přesně toto dělat, se dozvíte na EDUXové stránce kurzu BI-LIN.

Mnoho pěkných chvil při studiu lineární algebry přeje

Karel Klouda

Kapitola 1

Soustavy lineárních rovnic

Představte si, že někdo, kdo má hodně rychlou ruku a značné množství inkoustu, si udělal seznam všech matematických problémů a dělá si u každého čárku, kdykoli byl někde na světě a blízkém vesmíru řešen. Řešení soustav lineárních rovnic by se skoro jistě dostalo na stupně vítězů. Rozhodně by se tam dostalo, kdybychom vyřadili metody a výpočty, které se učí na základní škole.

Velice prozaickým důvodem pro to, proč je hledání řešení soustav lineárních rovnic tak často řešeným problémem, je to, že je to jeden z mála (matematických) problémů, které umíme vždy vyřešit. Navzdory častému přesvědčení toho v matematice zas tolik vyřešit neumíme. Měli byste již vědět, že stačí hledat kořeny polynomů (jedné proměnné) stupně pět a výše, a už můžeme mít neřešitelný problém. Kdybychom místo soustav lineárních rovnic uvažovali soustavy kvadratických rovnic, dostaneme také problém, který neumíme řešit. Fyzikální zákony, ale i např. ekonomické modely, mají většinou tvar (soustav) diferenciálních rovnic. Ani ty neumíme obecně uspokojivě vyřešit. U soustav lineárních rovnic jsme tedy v celkem mimořádné situaci, neboť je umíme vyřešit vždycky. Jediné, co nám může zabránit najít kompletní a přesné řešení je, že je rovnic příliš a my nemáme dostatečnou výpočetní sílu, nebo že nás zklamou nepřesně počítající počítače (přesné řešení nám zamlží nutné zaokrouhlovací chyby).

Co se vlastně myslí tím, že umíme vyřešit nějaký matematický problém? V předchozím odstavci jsme tím mysleli, že existuje rozumně rychlý algoritmus (nebo chcete-li výpočet), který umí najít přesné a kompletní řešení. Pro soustavy lineárních rovnic takové algoritmy existují. S jedním z nich se seznámíte již v této kapitole. Pro jiné jmenované problémy takové algoritmy buď neznáme, nebo dokonce víme, že neexistují. Samozřejmě existují postupy, jak se vypořádat s některými speciálními případy (např. některé diferenciální rovnice speciálního tvaru vyřešit umíme), ale my se teď bavíme o řešení ve vší obecnosti[1].

Teď byste mohli nabýt dojmu, že se např. fyzikové zabývají hledáním fyzikálních zákonů, které jsou nám na nic, protože je neumíme „vypočítat“. Není tomu tak: málokdy umíme najít přesné řešení, ale často umíme najít přibližné řešení dost blízké tomu přesnému, aby bylo užitečné. Metodám hledání těchto přibližných řešení

[1] Šťouravý čtenář by mohl namítnout, že soustavy lineárních rovnic jsou speciálním případem např. obecně neřešitelných soustav polynomiálních rovnic, a měl by pravdu. My si tím ale nebudeme kazit pointu tohoto lehkého úvodního zasvěcení.

(aproximací) se obecně říká numerické metody. Tyto metody často vypadají tak, že se pomocí nějakých sofistikovaných chytristik sestaví taková soustava lineárních rovnic, jejíž řešení nějakým způsobem dobře aproximuje řešení původního složitějšího problému.

Další ukázky reálných problémů, při jejichž řešení hrají soustavy lineárních rovnic klíčovou roli, potkáme později v tomto kurzu. Pokud ale čtenáře tento úvod i tyto ukázky aplikací nechají chladným, a učení se matematice považuje nezvratně za zbytečnost, chtěli bychom jej hned na začátku upozornit, že pro absolvování tohoto kurzu se porozumění problému řešení soustav lineárních rovnic považuje za naprosto nezbytné[2].

1.1 Co si z této kapitoly odneseme

1. Osvěžíme si relevantní znalosti ze střední školy, tedy schopnost řešit soustavy až tří rovnic o dvou až třech neznámých.

2. Soustavy o dvou či třech neznámých lze velmi názorně geometricky interpretovat, a tuto interpretaci si také oživíme.

3. Seznámíme se s pojmem *matice* a naučíme se matice sčítat a násobit.

4. Uvidíme, jak lze soustavy rovnic chápat jako matice.

5. Seznámíme se s Gaussovou *eliminační metodou* a pochopíme, co je horní stupňovitý tvar soustavy (resp. matice), a proč je pro řešení klíčový.

6. Pomocí Gaussovy eliminační metody se naučíme rozhodnout, kdy má soustava řešení a kdy je toto řešení jediné.

7. Seznámíme se s pojmem *tělesa* a několika příklady těles.

8. Ukážeme si, že většina toho, co platilo pro soustavy rovnic s reálnými proměnnými, platí i pro libovolné jiné těleso.

1.2 Staré známé soustavy lineárních rovnic

Soustava jedné lineární rovnice?

Nejjednodušší soustavou lineárních rovnic je soustava jedné rovnice o jedné (reálné) neznámé:

$$ax = b, \tag{1.1}$$

kde x je neznámé reálné číslo, a a b jsou též reálná čísla a a je navíc nenulové. Tato rovnice má vždy právě jedno řešení $x = a^{-1}b$ a všichni to vědí, takže můžeme jít dál.

My ovšem dál nepůjdeme a i když Vás to možná lehce urazí, u lineární rovnice jedné proměnné se zastavíme. Důvody pro to jsou dva. První je ten, že metodu pro

[2]Zde nechť si laskavý čtenář představí opravdu nesmlouvavý a přísný pohled zkoušejícího.

řešení soustav lineárních rovnic, se kterou se brzy seznámíme, lze chápat jako převod problému řešení soustavy rovnic na problém řešení několika rovnic tvaru (1.1).

Druhý důvod je pojem tělesa. Těleso bude pro mnohé čtenáře první (netriviální) abstraktní strukturou, kterou potká. Těleso budeme definovat pomocí pojmu *grupy*, což je další abstraktní struktura. Grupu můžeme do jisté míry chápat jako minimální strukturu, ve které má lineární rovnice jedné neznámé vždy řešení, které je navíc určeno jednoznačně[3]. Těleso pak můžeme v podobném duchu chápat jako minimální strukturu, kde umíme řešit soustavy lineárních rovnic.

Vyslovme tedy slavnostně první větu tohoto textu:

Věta 1.1. *Nechť $a, b \in \mathbb{R}$ a $a \neq 0$. Potom $x = a^{-1}b$ je jediné reálné číslo splňující rovnici $ax = b$.*

Než vyslovíme důkaz, řekneme si něco ke znění této věty. Matematická věta má obvykle dvě části. Tou první je vyslovení předpokladů, které můžeme chápat jako obdobu inicializace proměnných při psaní programu. Každý symbol použitý ve větě, musí mít určený význam: zde jsme jasně řekli, že a, b a x jsou reálná čísla s tím, že a je navíc nenulové. Výjimkou jsou symboly (zde například množina reálných čísel $\mathbb{R}$, exponent -1, rovnítko $=$, atp.), které se v kontextu považují za známé[4]. Druhou částí věty je výrok (z kurzu matematické logiky víte, co to přesně znamená), o kterém v důkazu prokážeme, že je pravdivý. K důkazu využíváme předpoklad, předchozí dokázané výroky a definice používaných pojmů.

Důkaz. Nejprve ukážeme, že $x = a^{-1}b$ je skutečně řešením rovnice $ax = b$ a to prostě tak, že za x dosadíme, a využijeme vlastností reálných čísel a jejich násobení:

$$a(a^{-1}b) = (aa^{-1})b = 1b = b.$$

První rovnítko jsme si mohli dovolit napsat díky tomu, že násobení reálných čísel je *asociativní*[5]. Druhé rovnítko je ospravedlněno tím, že každé nenulové reálné číslo a má *oboustrannou inverzi*, značenou obvykle a^{-1}, pro kterou platí $aa^{-1} = 1 = a^{-1}a$. Poslední rovnítko stojí na jedinečné vlastnosti (*neutralitě*) čísla 1: pro jakékoli reálné číslo c platí, že $1c = c$. Žádné jiné reálné číslo takovou vlastnost nemá.

Zbývá ukázat, že $x = a^{-1}b$ je jediné řešení. Důkaz jednoznačnosti už nebudeme tolik pitvat, neboť se využívají stejné vlastnosti jako výše. Předpokládejme, že x' je také řešení dané rovnice. Potom platí:

$$\begin{aligned}
ax' &= b && \text{// vynásob inverzním prvkem } a^{-1} \text{ zleva}\\
a^{-1}(ax') &= a^{-1}b && \text{// přesuň závorky (asociativita)}\\
(a^{-1}a)x' &= a^{-1}b && \text{// pro každé } a \text{ je } a^{-1}a = 1\\
1x' &= a^{-1}b && \text{// pro každé } c \text{ je } 1c = c\\
x' &= a^{-1}b.
\end{aligned}$$

[3] Předem upozorňujeme, že tato věta **není** definicí grupy a že pokud se ji za definici grupy pokusíte v písemce vydávat, vysloužíte si od opravujícího nula bodů a oči v sloup. Tato věta má usnadnit pochopení, sama o sobě ale grupu nedefinuje. Sami asi cítíte, že zatím nevíte, co to grupa je. Řádná definice přijde později v této kapitole.

[4] Ne, neexistuje žádný seznam takových „implicitně známých symbolů“. Předpokládáme, že čtenář je člověk, který prošel standardním vzděláním, a ne počítač, kterému se všechno musí explicitně napsat.

[5] Jestli nevíte, co to je asociativní, komutativní a distributivní zákon, tak si to honem někde zjistěte!

Ukázali jsme, že má-li rovnice $ax = b$ nějaké řešení, je tímto řešením právě a jen číslo $a^{-1}b$. Důkaz je tak hotov. $\square$

I když už se této triviální větě věnujeme (zdánlivě) neadekvátně dlouho, ještě si zdůrazněme jednu věc. Abychom větu dokázali, potřebovali jsme právě čtyři následující vlastnosti reálných čísel a jejich násobení:

1. Za samozřejmé jsme považovali, že součinem reálných čísel je opět reálné číslo.

2. Platnost asociativního zákona pro násobení.

3. Speciální vlastnost jedničky: pro všechna $c \in \mathbb{R}$ je $1c = c$.

4. Existenci inverze a^{-1} pro každé $a \neq 0$, a rovnosti $a^{-1}a = 1 = aa^{-1}$.

Všimněme si, že tyto čtyři vlastnosti má i množina $\mathbb{Q}$ racionálních čísel či množina $\mathbb{C}$ komplexních čísel. Naopak množina $\mathbb{Z}$ celých čísel už všechny tyto vlastnosti nemá: např. číslo 3 nemá v množině celých čísel inverzi.

Uf. Takže jsme kvůli triviální rovnici popsali jednu stránku, co bude dál? Ještě si připomeneme dvě (snad) notoricky známé věci. Ta první je, že jedna lineární rovnice o dvou neznámých $x, y \in \mathbb{R}$

$$ax + by = c, \quad a, b, c \in \mathbb{R}$$

definuje (mimo triviální případ $a = b = 0$) přímku v rovině $\mathbb{R}^2$ (pro jistotu: $\mathbb{R}^2$ je množina uspořádaných dvojic reálných čísel, neboli kartézský součin $\mathbb{R} \times \mathbb{R}$).

Poznámka 1.2. *Poznamenejme, že i např. rovnici $3x = 2$ lze prohlásit za rovnici dvou neznámých, kterou chápeme jako $3x + 0y = 2$. I pro tuto rovnici platí, že množina jejích řešení tvoří přímku v $\mathbb{R}^2$; je to přímka $x = 2/3$, tedy kolmice na osu x protínající ji v bodě $x = 2/3$.*

Podobně jako rovnice dvou neznámých definuje přímku v $\mathbb{R}^2$, definuje rovnice tří neznámých $x, y, z \in \mathbb{R}$

$$ax + by + cz = d, \quad a, b, c, d \in \mathbb{R}$$

rovinu v prostoru $\mathbb{R}^3$. Jedinou výjimkou je podobně jako výše případ $a = b = c = 0$, kdy je buď množina řešení prázdná (když $d \neq 0$) nebo je množinou řešení celé $\mathbb{R}^3$.

1.3 Geometrická interpretace množiny řešení

Vyvrcholením naší snahy porozumět problému hledání řešení soustav lineárních rovnic bude Frobeniova věta, která nám řekne, jak přesně množina řešení vypadá a s dalšími poznatky i umožní, tuto množinu přesně popsat. Než se k formulaci Frobeniovy věty dostaneme, musíme probrat mnoho pojmů. Už nyní si ale můžeme naznačit, jaké vlastnosti množina řešení soustavy rovnic může mít. Ve vší obecnosti budeme uvažovat soustavu m rovnic o n neznámých (n a m jsou přirozená čísla) a to nad libovolným tělesem. Jak ale později uvidíme, všechny možnosti toho, jak množina řešení může vypadat, lze demonstrovat už na jednoduchém (a představitelném) případě rovnic o třech neznámých.

Z Frobeniovy věty nám vyplyne, že existují tři možnosti: soustava nemá žádné řešení, má právě jedno anebo jich má nekonečně mnoho (alespoň tedy nad nekonečnými[6] tělesy). Ukážeme si příklady všech těchto možností.

Uvažme soustavu dvou rovnic o třech neznámých:

$$\begin{aligned} 2x + y - z &= 3, \\ 2x + y - z &= 4. \end{aligned} \tag{1.2}$$

Jelikož jsou obě levé strany rovnic stejné, nemohou se pro žádnou trojici $(x, y, z) \in \mathbb{R}^3$ rovnat současně 3 i 4, a proto žádné řešení této soustavy neexistuje.

Pro soustavu tří rovnic o třech neznámých

$$\begin{aligned} 3x + 2y + z &= 6, \\ 2y + z &= 3, \\ z &= 1, \end{aligned} \tag{1.3}$$

zjevně platí, že má jediné řešení $(1, 1, 1)$. Skutečně, stačí totiž použít větu 1.1: Má-li být (x, y, z) řešení, musí platit $z = 1$. Je-li $z = 1$, přechází druhá rovnice na jedinou rovnici jedné neznámé $2y = 2$ a ta má jediné řešení $y = 1$. Podobně zjistíme, že první rovnice nám po dosazení za y a z říká, že $x = 1$.

Když se na rovnice podíváme jako na rovnice tří rovin, můžeme říci, že řešením soustavy jsou body $\mathbb{R}^3$, které leží v průniku všech těchto tří rovin. Jak to vypadá, je vykresleno na obrázku 1.1.

Soustavu rovnic

$$\begin{aligned} 3x + 2y + z &= 6, \\ 2y + z &= 3, \\ 3x + 6y + 3z &= 12, \end{aligned} \tag{1.4}$$

zatím nebudeme přímo řešit, ale díky obrázku 1.2 vidíme, že průnik, a tedy i množina řešení, tvoří v $\mathbb{R}^3$ přímku. Když se podíváme podrobněji na rovnice (1.4), můžeme si všimnout, že poslední rovnice je vlastně součtem první a dvojnásobku druhé rovnice. Je tedy jasné, že pokud nějaký bod $(x, y, z) \in \mathbb{R}$ řeší první a druhou rovnici, musí nutně řešit i tu třetí a třetí rovnice je v systému vlastně zbytečná. Systém (1.4) má pak nutně množinu řešení shodnou se systémem

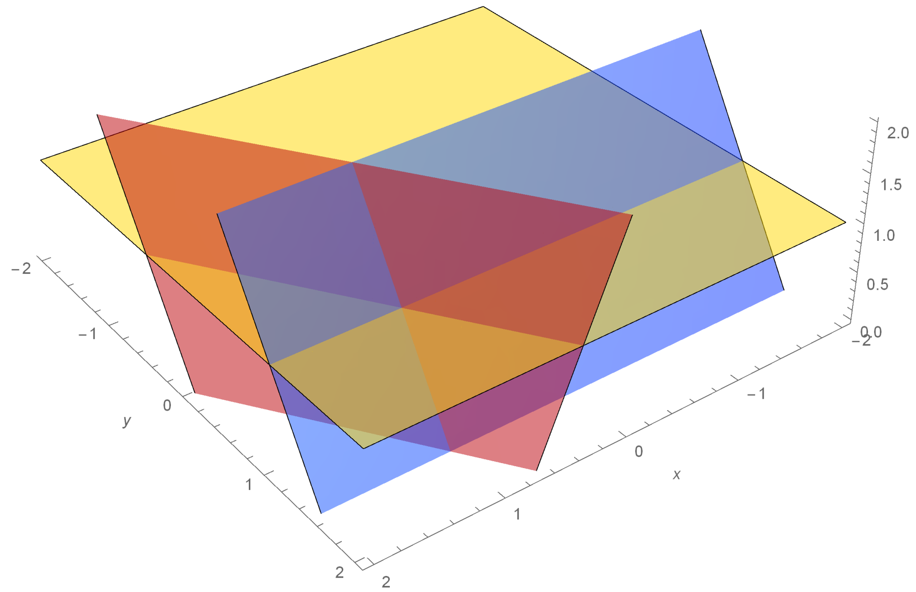
$$\begin{aligned} 3x + 2y + z &= 6, \\ 2y + z &= 3, \end{aligned}$$

neboli s průnikem dvou rovin. A průnik dvou rovin, pokud nejsou rovnoběžné, je vždy přímka.

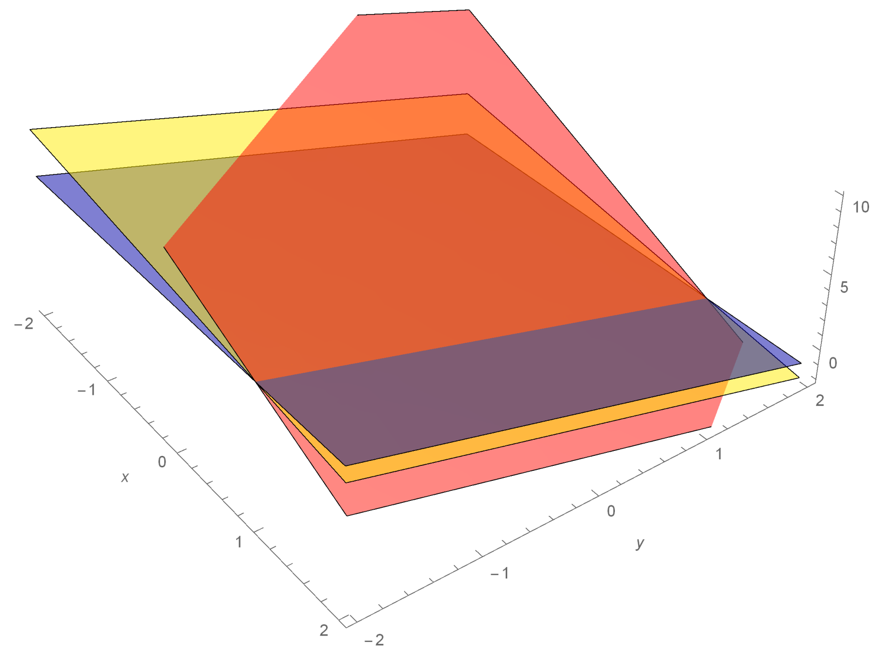
Poslední (poněkud triviální) případ, který může nastat, demonstruje tato soustava

$$\begin{aligned} 3x + 2y + z &= 6, \\ 6x + 4y + 2z &= 12, \\ 9x + 6y + 3z &= 18. \end{aligned}$$

[6] Nekonečné těleso je těleso mající nekonečně mnoho prvků. Např. tedy $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{C}$.



Obrázek 1.1: Vizualizace systému rovnic (1.3). První rovnice je vykreslena červeně, druhá modře a třetí žlutě.



Obrázek 1.2: Vizualizace systému rovnic (1.4). První rovnice je vykreslena červeně, druhá modře a třetí žlutě.

I méně pozorný čtenář si všimne, že druhá rovnice je dvojnásobkem a třetí trojnásobkem rovnice první. Proto pro libovolné řešení první rovnice musí nutně platit, že je současně řešením rovnice druhé i třetí a že tento systém vlastně odpovídá systému jedné rovnice $3x + 2y + z = 6$ a geometricky je to tedy rovina.

Viděli jsme na čtyřech příkladech, že už pro soustavy rovnic o třech neznámých mohou nastat situace, kdy řešení neexistuje, je právě jedno anebo je jich nekonečně mnoho. V případě nekonečně mnoha řešení navíc můžeme dostat přímku (jednodimenzionální[7] množinu) nebo rovinu (dvoudimenzionální množinu). Jak si snadno rozmyslíme, jiné případy u průniku rovin v $\mathbb{R}^3$ ani nastat nemohou. Co je překvapivější, že o moc více se nemůže stát ani v ($n$dimenzionálním) prostoru $\mathbb{R}^n$, když budeme uvažovat soustavy rovnic o n neznámých pro libovolné přirozené n.

1.4 Definice soustavy lineárních rovnic a snadno řešitelný případ

Opusťme již středoškolský prostor $\mathbb{R}^3$ a definujme si řádně pojem soustavy lineárních rovnic.

Definice 1.3. *Nechť n a m jsou přirozená čísla a pro všechna $i \in \{1, \ldots, m\}$ a $j \in \{1, \ldots, n\}$ platí, že $a_{ij} \in \mathbb{R}$ a $b_i \in \mathbb{R}$. Systém rovnic*

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ \vdots & & \vdots & & \ddots & & \vdots & = & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n & = & b_m \end{array} \tag{1.5}$$

nazýváme ***soustavou** m **lineárních rovnic o** n **neznámých**[8] $x_1, \ldots, x_n \in \mathbb{R}$. Číslu a_{ij} říkáme j**tý koeficient** i**té rovnice**.*

*Množinu všech uspořádaných ntic $(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$, pro které po dosazení do (1.5) je splněno všech m rovnic, nazýváme **množinou řešení soustavy** a značíme ji S.*

*Platí-li $b_1 = b_2 = \cdots = b_m = 0$, říkáme, že soustava (1.5) je **homogenní**. Není-li soustava homogenní, je **nehomogenní**[9].*

Přestože se v definici objevuje cizí slovo, neměla by čtenáře moc ničím zaskočit a tím pádem ani obohatit. Přesto si jako lehkou intelektuální rozcvičku uveďme následující jednoduchá pozorování, nad kterými by se čtenář měl zamyslet a sám sobě vysvětlit, proč jsou pravdivé[10].

Pozorování 1.4. *Následující pozorování se týkají soustavy rovnic (1.5), z definice 1.3 je přebráno i značení.*

[7] Pojem dimenze zatím chápejme intuitivně, přesný význam mu dáme později.

[8] Jelikož v tomto textu budeme mluvit téměř výhradně o soustavách lineárních rovnic, budeme pro zkrácení někdy mluvit prostě o soustavách, pokud nebude hrozit nedorozumění.

[9] Jak šokující.

[10] Udělejte to! Bude hůř a na horší časy je třeba mít natrénováno.

(i) *Číslo* a_{ij} *je číslo, kterým se násobí proměnná* x_j *v ité rovnici*[11].

(ii) *Množina řešení soustavy je rovna průniku množin řešení jednotlivých rovnic*[12].

(iii) *Homogenní soustava má vždy alespoň jedno řešení* $(0, 0, \dots, 0) \in \mathbb{R}^n$.

(iv) $(0, 0, \dots, 0) \in \mathbb{R}^n$ *není nikdy řešení nehomogenní soustavy rovnic.*

(v) *Je-li* $(x_1, x_2, \dots, x_n) \in \mathbb{R}^n$ *řešení homogenní soustavy, pak pro libovolné* $\alpha \in \mathbb{R}$ *je* $(\alpha x_1, \alpha x_2, \dots, \alpha x_n) \in \mathbb{R}^n$ *také řešení.*

(vi) *Předchozí tvrzení můžeme přepsat do následujícího tvaru:*

$$\forall \alpha \in \mathbb{R}, \forall (x_1, x_2, \dots, x_n) \in \mathbb{R}^n : \Big((x_1, x_2, \dots, x_n) \in S \Rightarrow \\ \Rightarrow (\alpha x_1, \alpha x_2, \dots, \alpha x_n) \in S \Big),$$

kde S *je množina řešení homogenní soustavy.*

(vii) *Má-li homogenní soustava i jiné řešení než* $(0, 0, \dots, 0) \in \mathbb{R}^n$*, pak má nekonečně mnoho řešení.*

Jediné pozorování, které lehce okomentujeme, je pozorování *(v)*. Ukážeme, že platí pro soustavy, kde $m = 1$, neboli pro jednu rovnici. Platnost pro libovolné soustavy pak plyne[13] z pozorování *(ii)*. Nechť tedy pro nějaké $(x_1, x_2, \dots, x_n) \in \mathbb{R}^n$ platí

$$a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0.$$

Díky tomu, že pro sčítání a násobení reálných čísel platí distributivní zákon (tj. můžeme vytýkat před závorku), můžeme psát

$$a_{11}\alpha x_1 + a_{12}\alpha x_2 + \dots + a_{1n}\alpha x_n = \alpha(a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n) = \alpha 0 = 0,$$

a tedy i $(\alpha x_1, \alpha x_2, \dots, \alpha x_n) \in \mathbb{R}^n$ je řešení.

Když už tedy máme definovanou soustavu lineárních rovnic, můžeme konečně přistoupit k otázce, jak najít její řešení. Již jsme si mohli na dříve uvedených příkladech všimnout, že některé soustavy se dají řešit snadno a některé ne. Uvažujme například soustavy

$$\begin{aligned} 3x + 2y + z &= 6 \\ 2y + z &= 3 \\ z &= 1 \end{aligned} \qquad \text{a} \qquad \begin{aligned} 3x + 2y + z &= 6 \\ 3x + 6y + 4z &= 13 \\ 4y + 2z &= 6. \end{aligned} \tag{1.6}$$

První soustavu už jsme řešili výše (je totožná s (1.3)) a zjistili jsme, že díky speciálnímu tvaru rovnic ji umíme vyřešit pomocí řešení tří lineárních rovnic pro jednu

[11] Toto uvádíme, abychom upozornili na konvenci, že se index **ř**ádku/rovnice píše jako první a index **s**loupce/proměnné jako druhý. Tuto konvenci budeme držet i u matic. Mnemotechnická pomůcka: je to podle abecedy (**ř** → **s**).

[12] I jednu rovnici lze chápat jako soustavu rovnic, takže pojem množina řešení je dobře definován i pro jednotlivé rovnice.

[13] To si také rozmyslete a pochopte!

neznámou. Získali jsme jediné řešení $(1,1,1)$. S využitím zavedeného značení tedy pro tuto soustavu platí $S = \{(1,1,1)\}$. Jak snadno ověříme, pro druhou soustavu rovnic je $(1,1,1)$ také řešení, není ale už tak snadno vidět, jak na toto řešení přijít a ani jestli je jediné.

Jak vidno, některé soustavy mají tvar, který umožňuje snadné hledání množiny řešení a jiné soustavy nikoli. Pro hledání řešení by tedy bylo velice užitečné, pokud bychom soustavou mohli upravit tak, že bychom ji dostali do toho „vyřešitelného tvaru“, aniž bychom změnili množinu řešení. A jak uvidíme, máme štěstí, takové úpravy existují. Jsou dokonce velice jednoduché (opět používáme značení z definice 1.3):

(U1) Prohození dvou rovnic.

(U2) Vynásobení jedné rovnice nenulovým číslem, přesněji výměna rovnice

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = b_i$$

rovnicí

$$a_{i1}\alpha x_1 + a_{i2}\alpha x_2 + \cdots + a_{in}\alpha x_n = \alpha b_i$$

pro nějaké $1 \leq i \leq m$ a $\alpha \in \mathbb{R} \setminus \{0\}$.

(U3) Přičtení libovolného násobku jedné rovnice k jiné rovnici, přesněji nahrazení rovnice

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = b_i$$

za rovnici

$$(a_{i1} + \alpha a_{j1})x_1 + (a_{i2} + \alpha a_{j2})x_2 + \cdots + (a_{in} + \alpha a_{jn})x_n = b_i + \alpha b_j$$

pro nějaká *různá* čísla $i, j \in \{1, 2, \ldots, m\}$ a $\alpha \in \mathbb{R}$.

Ukažme si nyní, že pomocí těchto tří úprav umíme převést pravou soustavu z (1.6) na tu levou:

$$\begin{aligned} 3x + 2y + z &= 6 \\ 3x + 6y + 4z &= 13 \\ 4y + 2z &= 6 \end{aligned} \quad \xrightarrow[r2-r1]{U3} \quad \begin{aligned} 3x + 2y + z &= 6 \\ 4y + 3z &= 7 \\ 4y + 2z &= 6 \end{aligned} \quad \xrightarrow[r2-r3]{U3}$$

$$\begin{aligned} 3x + 2y + z &= 6 \\ z &= 1 \\ 4y + 2z &= 6 \end{aligned} \quad \xrightarrow[r2\leftrightarrow r3]{U1} \quad \begin{aligned} 3x + 2y + z &= 6 \\ 4y + 2z &= 6 \\ z &= 1 \end{aligned} \quad \xrightarrow[\frac{1}{2}\cdot r2]{U2}$$

$$\begin{aligned} 3x + 2y + z &= 6 \\ 2y + z &= 3 \\ z &= 1. \end{aligned} \tag{1.7}$$

Popisky u šipek naznačují, jakou úpravu jsme použili: např. $\xrightarrow[r2-r3]{U3}$ značí, že jsme použili úpravu (U3), konkrétně jsme k druhé rovnici přičetli -1 násobek rovnice třetí[14]. Upravovat soustavy rovnic tedy umíme, co je ale důležité, že všech pět soustav uvedených výše má stejné množiny řešení! A jelikož množinu řešení finální soustavy známe, je to $S = \{(1,1,1)\}$, známe i řešení všech předchozích. Zbývá nám jenom ukázat, že to opravdu funguje.

Věta 1.5. *Převedeme-li jednu soustavu lineárních rovnic na jinou pomocí jedné z úprav (U1), (U2) nebo (U3), mají obě soustavy stejnou množinu řešení.*

Důkaz. Z definice množiny řešení (viz definice (1.3)) je jasné, že prohození rovnic na tuto množinu nemá žádný vliv, a tvrzení věty pro úpravu (U1) tedy platí.

Dále ukážeme, že změníme-li jednu rovnici pomocí úpravy (U2), množina řešení této jedné rovnice se nezmění. Že se nezmění ani množina řešení soustavy je pak zřejmé (viz bod *(ii)* v pozorování 1.4). Chceme vlastně ukázat, že množina řešení $i$té rovnice (používáme stále značení z definice 1.3 a z definice úprav (U1 – U3) výše)

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = b_i,$$

pro nějaké $1 \le i \le m$, je stejná jako množina řešení rovnice

$$a_{i1}\alpha x_1 + a_{i2}\alpha x_2 + \cdots + a_{in}\alpha x_n = \alpha b_i$$

pro libovolné nenulové $\alpha \in \mathbb{R}$. Díky distributivitě sčítání a násobení reálných čísel víme, že

$$a_{i1}\alpha x_1 + a_{i2}\alpha x_2 + \cdots + a_{in}\alpha x_n = \alpha(a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n) = \alpha b_i.$$

A jelikož v reálných číslech je rovnice $\alpha y = \alpha z$ pro nenulové α ekvivalentní s rovnicí $y = z$, je důkaz pro (U2) hotov[15].

Pro úpravu (U3) postupujeme stejně jako pro (U2): díky $j$té rovnici soustavy, která říká, že

$$a_{j1}x_1 + a_{j2}x_2 + \cdots + a_{jn}x_n = b_j$$

plyne z rovnosti

$$\begin{aligned}(a_{i1} + \alpha a_{j1})x_1 + (a_{i2} + \alpha a_{j2})x_2 + \cdots + (a_{in} + \alpha a_{jn})x_n &= \\ = (a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n) + \alpha(a_{j1}x_1 + a_{j2}x_2 + \cdots + a_{jn}x_n) &= \\ &= b_i + \alpha b_j,\end{aligned}$$

že platí

$$(a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n) + \alpha b_j = b_i + \alpha b_j.$$

Tato rovnice má zřejmě stejnou množinu řešení jako rovnice

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = b_i.$$ □

[14] Lidštěji řečeno, odečetli jsme od druhé rovnice tu třetí.

[15] Tím, že zde vypisujeme takovéto (zřejmé) důvody proto, proč něco platí, se snažíme čtenáři ukázat, jak by měl uvažovat. Výhledově takto podrobného vysvětlování ubude, protože doufáme, že jej dostanete pod kůži.

1.5 Matice a základní operace s nimi

V této sekci si zavedeme jeden z nejdůležitějších pojmů lineární algebry: pojem matice. Nejedná se o nic složitého (jsou to vlastně jen čísla zapsaná do obdélníku), což je dobře, neboť se s tímto pojmem budete potkávat často i během dalšího studia a nejen v matematických předmětech. Pro nás je ale akutní motivace velice prozaická: chceme si zjednodušit značení soustavy lineárních rovnic.

Zjednodušení spočívá v zavedení konvence, která určuje význam koeficientu podle jeho polohy, což umožňuje vyhnout se opakovanému psaní názvů proměnných. Uveďme příklad tohoto zjednodušeného zápisu:

$$\begin{aligned} 3x + 2y + z &= 6 \\ 3x + 6y + 4z &= 13 \\ 4y + 2z &= 6 \end{aligned} \quad \text{budeme zapisovat jako} \quad \left(\begin{array}{ccc|c} 3 & 2 & 1 & 6 \\ 3 & 6 & 4 & 13 \\ 0 & 4 & 2 & 6 \end{array}\right). \tag{1.8}$$

Pokud není řečeno jinak, sloupce odpovídají pořadí proměnných podle abecedy či indexu, tedy první sloupec odpovídá x (resp. x_1), druhý y (resp. x_2) atd.

Definice 1.6. *Nechť $m, n \in \mathbb{N}$. Uspořádaný soubor mn čísel zapsaný do tabulky*[16] *o m řádcích a n sloupcích nazýváme* ***matice*** *typu $m \times n$. Matice obvykle značíme takto:*

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

kde a_{ij} jsou ***prvky*** *matice (někdy je značíme taky jako $\mathbb{A}_{ij}$ a nazýváme je ij**té prvky**). Číslu i říkáme* ***řádkový*** *a číslu j* ***sloupcový*** *index.*

Množinu všech matic typu *$m \times n$ (s reálnými prvky) značíme $\mathbb{R}^{m,n}$. Jako $\mathbb{A}_{:j} \in \mathbb{R}^{m,1}$ značíme j**tý sloupec** matice $\mathbb{A}$:*

$$\mathbb{A}_{:j} = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}.$$

*Podobně $\mathbb{A}_{i:} \in \mathbb{R}^{1,n}$ značí i**tý řádek** matice $\mathbb{A}$:*

$$\mathbb{A}_{i:} = \begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \end{pmatrix}.$$

Dvě matice se rovnají, pokud jsou stejného typu a mají shodné všechny odpovídající prvky.

Nyní si zavedeme čtyři základní operace, které budeme dále hojně využívat. Je to násobení matice číslem, sčítání dvou matic, transponování matice a násobení dvou matic. Z těchto operací již snadno odvodíme odčítání (což je vlastně přičítání (-1) násobku) a např. mocnění $\mathbb{A}^3 = \mathbb{A} \cdot \mathbb{A} \cdot \mathbb{A}$).

[16] Do dvourozměrného pole, chcete-li.

Násobení matice číslem a sčítání matic

Jak násobení matice číslem tak sčítání matic bude definováno tzv. „po prvcích“. Pro matice typu $m \times n$ to tedy bude odpovídat mn nezávislých násobení dvou reálných čísel resp. mn nezávislých sčítání dvou reálných čísel. Při sčítání po prvcích musíme mít ke každému prvku jedné matice odpovídající prvek druhé matice (musí být ve stejném řádku i sloupci), a proto umíme sčítat pouze matice stejného typu.

Definice 1.7. *Buďte $m, n \in \mathbb{N}$, $\alpha \in \mathbb{R}$ a $\mathbb{A}, \mathbb{B} \in \mathbb{R}^{m,n}$ matice s prvky a_{ij} resp. b_{ij}. Součin matice $\mathbb{A}$ a reálného čísla α definujeme takto:*

$$\alpha\mathbb{A} := \begin{pmatrix} \alpha a_{11} & \alpha a_{12} & \cdots & \alpha a_{1n} \\ \alpha a_{21} & \alpha a_{22} & \cdots & \alpha a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha a_{m1} & \alpha a_{m2} & \cdots & \alpha a_{mn} \end{pmatrix}.$$

Součet matic $\mathbb{A}$ a $\mathbb{B}$ definujeme jako

$$\mathbb{A} + \mathbb{B} := \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \cdots & a_{mn} + b_{mn} \end{pmatrix}.$$

Matici $\mathbb{A} + (-1)\mathbb{B}$ nazýváme rozdíl matice $\mathbb{A}$ a $\mathbb{B}$ a značíme $\mathbb{A} - \mathbb{B}$, matici $(-1)\mathbb{A}$ značíme jako $-\mathbb{A}$.

Uveďme opět několik pozorování, které si laskavý čtenář sám promyslí (tj. dokáže) a sám sobě vysvětlí, proč jsou pravdivá. Většina z nich plyne z toho, co bylo řečeno před předchozí definicí, tedy že definice operací po prvcích vlastně znamená, že se jedná o mn nezávislých (ale uspořádaných) operací s dvěma reálnými čísly.

Pozorování 1.8. *Buďte $m, n \in \mathbb{N}$, $\alpha \in \mathbb{R}$ a $\mathbb{A}, \mathbb{B} \in \mathbb{R}^{m,n}$ matice s prvky a_{ij} resp. b_{ij}.*

1. *Matice $\alpha\mathbb{A}$ i $\mathbb{A} + \mathbb{B}$ jsou opět prvky $\mathbb{R}^{m,n}$, neboli násobení číslem ani sčítání matic nemění počet řádků ani počet sloupců.*

2. *Jelikož je sčítání reálných čísel komutativní, je i sčítání matic komutativní. Platí tedy*
$$\mathbb{A} + \mathbb{B} = \mathbb{B} + \mathbb{A}.$$

3. *Jelikož sčítání a násobení reálných čísel splňuje distributivní zákon, je distributivní i operace násobení matic číslem vůči maticovému sčítání. Přesněji, platí rovnost*
$$\alpha(\mathbb{A} + \mathbb{B}) = \alpha\mathbb{A} + \alpha\mathbb{B}.$$

4. *Pro všechna přirozená čísla n platí*
$$n\mathbb{A} = \underbrace{\mathbb{A} + \mathbb{A} + \cdots + \mathbb{A}}_{n\text{krát}}.$$

5. *Jelikož rovnice $a + x = b$, pro reálná čísla $a, b \in \mathbb{R}$ a reálnou neznámou x, má jediné řešení $x = -a + b$, má i rovnice*

$$\mathbb{A} + \mathbb{X} = \mathbb{B}$$

s neznámou maticí $\mathbb{X} \in \mathbb{R}^{m,n}$ jediné řešení $\mathbb{X} = -\mathbb{A} + \mathbb{B} = (-1)\mathbb{A} + \mathbb{B}$.

Transponovaná matice

Transpozice matice není aritmetická operace, ale spíše jakési přeskládání prvků. Jelikož se často provádí, zavádí se pro ni speciální značení.

Definice 1.9. *Buďte $m, n \in \mathbb{N}$ a $\mathbb{A} \in \mathbb{R}^{m,n}$ matice s prvky a_{ij}. **Transpozicí** matice $\mathbb{A}$ nazýváme matici z $\mathbb{R}^{n,m}$, jejíž prvek v $j$tém řádku a $i$tém sloupci je roven a_{ij}. Tuto matici značíme $\mathbb{A}^T$.*

Transponování tedy vlastně znamená, že vezmeme řádky matice $\mathbb{A}$ a zapíšeme je do sloupců (při zachovaném pořadí).

Příklad 1.10. *Platí následující:*

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^T = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} \quad a \quad \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}^T = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}.$$

Pro každou matici $\mathbb{A}$ také platí $(\mathbb{A}^T)^T = \mathbb{A}$.

Násobení matic

Násobení matice maticí bude pro mnohé z čtenářů první zásadnější novinkou[17]. Je proto možné, že při prvním pohledu na definici si některý čtenář pomyslí „Proč zrovna takhle?“. Už brzy uvidíme, že zvolená definice násobení má např. tu výhodu, že pomocí ní budeme moci zjednodušit značení pro soustavu rovnic (1.5) na jednoduchou (maticovou) rovnici $\mathbb{A}\mathbb{x} = \mathbb{b}$. To ale není zdaleka jediná výhoda a skutečný důvod, proč je součin matic definován takto, se dozvíte později[18].

Definice 1.11. *Buďte $m, n, p \in \mathbb{N}$, $\mathbb{A} \in \mathbb{R}^{m,n}$ matice s prvky a_{ij} a $\mathbb{B} \in \mathbb{R}^{n,p}$ matice s prvky b_{ij}. Součinem matic $\mathbb{A}$ a $\mathbb{B}$ je matice $\mathbb{D} \in \mathbb{R}^{m,p}$ s prvky d_{ij}, pro kterou platí*

$$d_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}, \tag{1.9}$$

značíme $\mathbb{D} = \mathbb{A}\mathbb{B}$.

[17] Samozřejmě ne pro ty nadšence, kteří kurz lineární algebry opakují.

[18] Pro nedočkavé: ukážeme si, že matice vlastně reprezentují všechna možná lineární zobrazení a že skládání lineárních zobrazení odpovídá právě námi definovanému násobení jejich maticových reprezentací.

V této definici je třeba věnovat pozornost každému písmenku. Například si všimneme, že matice $\mathbb{A}$ a $\mathbb{B}$ mohou být různého typu. Co se musí shodovat, je počet (označený jako n) sloupců matice $\mathbb{A}$ a počet řádků matice $\mathbb{B}$. Proč se musí tato dvě čísla shodovat je jasné ze sumy (1.9): sčítací index k nabývá hodnot od 1 do n a ve sčítancích $a_{ik}b_{kj}$ pak tento index hraje roli sloupcového indexu matice $\mathbb{A}$ a řádkového indexu matice $\mathbb{B}$.

Příklad 1.12. *Platí následující:*

$$\begin{pmatrix} 1 & 2 & -1 \\ 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & -1 \\ 4 & 5 & 6 & -1 \\ 1 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 8 & 11 & 14 & -3 \\ 2 & 3 & 4 & -1 \end{pmatrix}.$$

Například prvek 14 *ležící ve výsledné matici v prvním řádku a třetím sloupci získáme tak, že vezmeme první řádek* $\begin{pmatrix} 1 & 2 & -1 \end{pmatrix}$ *levé matice a třetí sloupec* $\begin{pmatrix} 3 & 6 & 1 \end{pmatrix}^T$ *pravé matice a sečteme výsledky součinů provedených „po prvcích“:*

$$1 \cdot 3 + 2 \cdot 6 + (-1) \cdot 1 = 14.$$

Součin matic *není obecně komutativní.* Může se dokonce stát, že součin $\mathbb{AB}$ je definován a $\mathbb{BA}$ není (vizte předchozí příklad). Ale i pokud oba součiny definovány jsou, násobení stejně není obecně komutativní, protože výsledky mohou být matice různého typu. A i když stejného typu jsou, nemusí si být rovny.

Příklad 1.13. *Platí následující*

$$\begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 6 \end{pmatrix},$$

tedy výsledkem násobení matice z $\mathbb{R}^{1,3}$ *maticí z* $\mathbb{R}^{3,1}$ *je matice z* $\mathbb{R}^{1,1}$*.*

Po prohození pořadí matic je výsledek z $\mathbb{R}^{3,3}$*:*

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

Aby násobení mohlo být vůbec komutativní, musíme se omezit na matice, které mají stejný počet řádků i sloupců. Jedná se o matice typu $n \times n$ a nazývají se ze zřejmého důvodu **čtvercové**. Pro čtvercové matice $\mathbb{A}, \mathbb{B} \in \mathbb{R}^{n,n}$ platí, že matice $\mathbb{AB}$ i matice $\mathbb{BA}$ jsou opět z $\mathbb{R}^{n,n}$. Je tedy komutativní alespoň násobení čtvercových matic? Není, jak je vidět na následujícím příkladě.

Příklad 1.14. *Platí následující:*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \quad a \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Komutativní tedy násobení matic obecně není, platí pro něj alespoň asociativní zákon? Ukážeme si, že platí, musíme se ale opět omezit na matice takových rozměrů, aby uvažované násobení bylo dobře definované.

Věta 1.15. *Nechť $m, n, s, t \in \mathbb{N}$. Pro libovolné matice $\mathbb{A} \in \mathbb{R}^{m,n}$, $\mathbb{B} \in \mathbb{R}^{n,s}$ a $\mathbb{D} \in \mathbb{R}^{s,t}$ platí*

$$\mathbb{A}(\mathbb{B}\mathbb{D}) = (\mathbb{A}\mathbb{B})\mathbb{D}.$$

Důkaz. V následujících rovnostech používáme definici maticového násobení a využíváme toho, že násobení reálných čísel je asociativní, a také toho, že pro sčítání a násobení reálných čísel platí distributivní zákon. Symbolem $(\mathbb{B}\mathbb{D})_{kj}$ značíme prvek matice $\mathbb{B}\mathbb{D}$ v $k$tém řádku a $j$tém sloupci. Ukážeme, že ijtý prvek matice $\mathbb{A}(\mathbb{B}\mathbb{D})$ je roven ijtému prvku matice $(\mathbb{A}\mathbb{B})\mathbb{D}$ pro libovolné $1 \le i \le m$ a $1 \le j \le t$:

$$\begin{aligned}
[\mathbb{A}(\mathbb{B}\mathbb{D})]_{ij} &= \sum_{k=1}^{n} \mathbb{A}_{ik}(\mathbb{B}\mathbb{D})_{kj} = \sum_{k=1}^{n} \mathbb{A}_{ik} \sum_{\ell=1}^{s} \mathbb{B}_{k\ell}\mathbb{D}_{\ell j} = \sum_{k=1}^{n}\sum_{\ell=1}^{s} \mathbb{A}_{ik}\mathbb{B}_{k\ell}\mathbb{D}_{\ell j} \\
&= \sum_{\ell=1}^{s}\sum_{k=1}^{n} \mathbb{A}_{ik}\mathbb{B}_{k\ell}\mathbb{D}_{\ell j} = \sum_{\ell=1}^{s}\left(\sum_{k=1}^{n} \mathbb{A}_{ik}\mathbb{B}_{k\ell}\right)\mathbb{D}_{\ell j} = \sum_{\ell=1}^{s} (\mathbb{A}\mathbb{B})_{i\ell}\mathbb{D}_{\ell j} \\
&= [(\mathbb{A}\mathbb{B})\mathbb{D}]_{ij}.
\end{aligned}$$

Protože jsme i, j volili libovolně, každý ijtý prvek matice $\mathbb{A}(\mathbb{B}\mathbb{D})$ je roven ijtému prvku matice $(\mathbb{A}\mathbb{B})\mathbb{D}$. Tedy $\mathbb{A}(\mathbb{B}\mathbb{D}) = (\mathbb{A}\mathbb{B})\mathbb{D}$. □

Ještě jednou zdůrazňujeme, že asociativitu násobení matic jsme dokázali pouze s využitím definice tohoto násobení[19] a s využitím asociativity násobení a distributivity násobení a sčítání reálných čísel.

Mohli bychom si vymyslet ještě mnoho různých vlastností maticového násobení, a proto to aspoň trochu uděláme:

Věta 1.16. *V následujících tvrzeních jsou rozměry matic $\mathbb{A}$, $\mathbb{B}$ a $\mathbb{D}$ vždy takové, aby obsažené výrazy měly smysl a $\alpha \in \mathbb{R}$. Platí:*

(i) $\mathbb{A}(\mathbb{B} + \mathbb{D}) = \mathbb{A}\mathbb{B} + \mathbb{A}\mathbb{D}$, *(distributivní zákon)*

(ii) $(\mathbb{A} + \mathbb{B})\mathbb{D} = \mathbb{A}\mathbb{D} + \mathbb{B}\mathbb{D}$, *(distributivní zákon)*

(iii) $\alpha(\mathbb{A}\mathbb{B}) = (\alpha\mathbb{A})\mathbb{B} = \mathbb{A}(\alpha\mathbb{B})$,

(iv) $(\mathbb{A}\mathbb{B})^T = \mathbb{B}^T\mathbb{A}^T$.

Větu dokazovat nebudeme, protože věříme, že si důkazy laskavý čtenář udělá sám. Vždy bude platit, že si vystačí s definicí násobení, transponování a sčítání matic, definicí násobení matice číslem a asociativitou, distributivitou a komutativitou[20] násobení a sčítání reálných čísel[21].

[19] Samozřejmě.

[20] Tu potřebujeme pro důkaz posledních dvou rovností.

[21] Opakujeme to pořád dokola záměrně, jestli budete ještě pár stránek číst, budete za to vděční! Pokud tedy nejste ten typ studentů, kterému se člověk nezavděčí.

Maticový zápis soustavy rovnic

Zkusme si teď jen tak vynásobit následující dvě matice:

$$\mathbb{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \in \mathbb{R}^{m,n} \quad \text{a} \quad \mathbb{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^{n,1}.$$

Vzhledem k tomu, že matice $\mathbb{A}$ má stejně sloupců jako matice $\mathbb{x}$ řádků, násobení půjde jako po másle. Výsledkem bude tato matice z $\mathbb{R}^{m,1}$:

$$\mathbb{A}\mathbb{x} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{pmatrix}.$$

Abychom se dostali k pointě, položíme si otázku, kdy se matice $\mathbb{A}\mathbb{x}$ rovná matici

$$\mathbb{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{R}^{m,1}.$$

Podle definice 1.6 se matice se rovnají, pokud jsou stejného typu (což je zde splněno, obě jsou typu $m \times 1$) a mají stejné všechny odpovídající prvky, proto rovnost $\mathbb{A}\mathbb{x} = \mathbb{b}$ nastává, právě když

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ \vdots & & \vdots & & \ddots & & \vdots & = & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n & = & b_m. \end{array}$$

V tom ale pozorný čtenář jistě poznává naší dobrou známou soustavu lineárních rovnic (1.5) z definice 1.3! Zápis $\mathbb{A}\mathbb{x} = \mathbb{b}$ je tedy naprosto ekvivalentním vyjádřením týchž rovností. Jelikož je mnohem elegantnější, budeme jej v dalším textu preferovat a pro jistotu si jeho pomocí (také) definujeme pojem soustavy lineárních rovnic[22]. Než ale přistoupíme k samotné definici, zavedeme si značení, které budeme hojně používat v následujícím textu.

Definice 1.17. *Nechť $m, n \in \mathbb{N}$. Prvky $\mathbb{R}^{m,1}$ budeme nazývat mprvkové* ***vektory*** *a namísto $\mathbb{R}^{m,1}$ budeme často psát pouze $\mathbb{R}^m$. Vektor z $\mathbb{R}^m$, jehož všechny prvky jsou nuly, budeme nazývat* ***nulový vektor*** *a značit θ. Matici z $\mathbb{R}^{m,n}$, jejíž všechny prvky jsou nuly, budeme nazývat* ***nulovou maticí*** *a značit Θ.*

[22]Je trochu neobvyklé, mít v jednom matematickém textu dvě definice téhož pojmu, i když jsou třeba ekvivalentní. Obvyklý postup je jednu si vybrat a o druhé dokázat, že je ekvivalentním vyjádřením téhož (v případě nejasností kontaktujte prosím odborníka na tuto problematiku Ing. Miroslava Hrončoka). V našem případě se ale nejedná ani o klasickou ekvivalenci, je to prostě to samé, jenom jinak označené. Proto si „prohřešek“ dvou definic dovolíme.

Z definice plyne, že $\mathbb{R}^m$ je množina $m$prvkových vektorů psaných „do sloupce“. Této konvence se budeme držet. Pokud budeme potřebovat zapsat vektor $\mathbb{x}$ do řádku, použijeme operaci transpozice $\mathbb{x}^T$.

Definice 1.18 (Maticový zápis soustavy lineárních rovnic)**.** *Nechť $m, n \in \mathbb{N}$, $\mathbb{A} \in \mathbb{R}^{m,n}$, $\mathbb{b} \in \mathbb{R}^m$. Rovnici*

$$\mathbb{A}\mathbb{x} = \mathbb{b} \tag{1.10}$$

nazýváme soustavou m lineárních rovnic pro n neznámých $x_1, x_2, \ldots, x_n$. Vektor

$$\mathbb{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

*nazýváme **vektorem neznámých** a vektor $\mathbb{b}^T = \begin{pmatrix} b_1 & b_2 & \cdots & b_m \end{pmatrix}$ vektorem **pravých stran**.*

*Matici $\mathbb{A}$ nazýváme **maticí soustavy** a matici*

$$(\mathbb{A} \mid \mathbb{b}) = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right)$$

rozšířenou maticí soustavy[23]*. Je-li $\mathbb{b} = \theta \in \mathbb{R}^m$, mluvíme o **homogenní soustavě**. Soustava $\mathbb{A}\mathbb{x} = \theta$ je **přidruženou homogenní soustavou lineárních rovnic** k soustavě $\mathbb{A}\mathbb{x} = \mathbb{b}$.*

Množinu všech řešení soustavy $\mathbb{A}\mathbb{x} = \mathbb{b}$ značíme S a množinu řešení přidružené homogenní soustavy S_0.

Struktura řešení soustavy

V pozorování 1.4 jsme si ukázali, že je-li $\mathbb{x}$ řešením homogenní soustavy $\mathbb{A}\mathbb{x} = \theta$, pak také $\alpha\mathbb{x}$ je jejím řešením pro libovolné $\alpha \in \mathbb{R}$. S využitím jednoduššího značení a vlastností násobení matic si můžeme ukázat o množině řešení další důležité věci.

Věta 1.19. *Uvažujme soustavu rovnic $\mathbb{A}\mathbb{x} = \mathbb{b}$. Platí následující:*

(i) Je-li $\mathbb{x} \in S_0$ a $\alpha \in \mathbb{R}$, je také $\alpha\mathbb{x} \in S_0$.

(ii) Je-li $\mathbb{x}, \mathbb{y} \in S_0$, je také $\mathbb{x} + \mathbb{y} \in S_0$.

(iii) Je-li $\mathbb{x}, \mathbb{y} \in S$, je $\mathbb{x} - \mathbb{y} \in S_0$.

(iv) Buď $\mathbb{x} \in S$, potom pro každý vektor $\mathbb{y} \in S$ existuje nějaký vektor $\mathbb{z} \in S_0$ tak, že $\mathbb{y} = \mathbb{x} + \mathbb{z}$.

[23] Svislá čára mezi posledním a předposledním sloupcem se používá pouze pro grafické zvýraznění toho, co považujeme za pravou stranu. Nemá žádný jiný význam a rozšířená matice soustavy je normální matice z $\mathbb{R}^{m,n+1}$.

(v) Buď $\mathbb{x} \in S$, potom pro každý vektor $\mathbb{z} \in S_0$ platí, že $\mathbb{x} + \mathbb{z} \in S$.

Důkaz. Tvrzení *(i)* už jsme dokázali dříve. Tvrzení *(ii)* je přímým důsledkem distributivního zákona (vizte větu 1.16, bod (i)) a zřejmého faktu, že $\theta + \theta = \theta$:

$$\mathbb{A}(\mathbb{x} + \mathbb{y}) = \mathbb{A}\mathbb{x} + \mathbb{A}\mathbb{y} = \theta + \theta = \theta,$$

tedy skutečně i $\mathbb{x} + \mathbb{y}$ řeší přidruženou homogenní soustavu a patří do množiny S_0.

Jelikož je $\mathbb{x} - \mathbb{y}$ definováno jako $\mathbb{x} + (-1)\mathbb{y}$, dostáváme s pomocí *(i)* a *(ii)* toto:

$$\mathbb{A}(\mathbb{x} - \mathbb{y}) = \mathbb{A}(\mathbb{x} + (-1)\mathbb{y}) = \mathbb{A}\mathbb{x} + \mathbb{A}((-1)\mathbb{y}) = \mathbb{A}\mathbb{x} + (-1)\mathbb{A}\mathbb{y} = \mathbb{A}\mathbb{x} - \mathbb{A}\mathbb{y}.$$

Můžeme tedy říci, že distributivní zákon platí pro násobení i vůči odčítání matic. Z předpokladu tvrzení *(iii)* $\mathbb{x}, \mathbb{y} \in S$ plyne, že $\mathbb{A}\mathbb{x} = \mathbb{A}\mathbb{y} = \mathbb{b}$, což s využitím předchozího výpočtu dává

$$\mathbb{A}(\mathbb{x} - \mathbb{y}) = \mathbb{A}\mathbb{x} - \mathbb{A}\mathbb{y} = \mathbb{b} - \mathbb{b} = \theta,$$

tedy skutečně $\mathbb{x} - \mathbb{y} \in S_0$.

Tvrzení *(iv)* je přímým důsledkem *(iii)*, neboť hledaný $\mathbb{z}$ je roven vektoru $\mathbb{y} - \mathbb{x}$, který je dle *(iii)* prvkem S_0 a zároveň zřejmě platí[24] $\mathbb{x} + (\mathbb{y} - \mathbb{x}) = \mathbb{y}$.

Tvrzení *(v)* je jen dalším důsledkem distributivního zákona a toho, že $\mathbb{b} + \theta = \mathbb{b}$:

$$\mathbb{A}(\mathbb{x} + \mathbb{z}) = \mathbb{A}\mathbb{x} + \mathbb{A}\mathbb{z} = \mathbb{b} + \theta = \mathbb{b}.$$

□

Zavedeme si ještě jeden pojem, který nám umožní zapsat tvrzení *(iv)* a *(v)* v elegantnějším a čitelnějším formátu:

Definice 1.20. *Buďte A a B libovolné podmnožiny nějaké množiny M, pro jejíž prvky je definováno sčítání $+ : M \times M \to M$ a násobení $\cdot : \mathbb{R} \times M \to M$ číslem z $\mathbb{R}$.* ***Součet množin*** *A a B definujeme následovně:*

$$A + B := \{a + b \mid a \in A, b \in B\}.$$

Je-li $A = \{a\}$ jednoprvková, píšeme $a + B$ namísto $\{a\} + B$.

Podobně ***součin reálného čísla*** *$\alpha \in \mathbb{R}$* ***a množiny*** *A definujeme jako*

$$\alpha A := \{\alpha a \mid a \in A\}.$$

Součet množin je tedy definován jako množina všech součtů všech různých dvojic prvků z obou množin. Možná Vás zaskočil ten podivný předpoklad, že „M je libovolná množina, pro jejíž prvky je definováno sčítání $+ : M \times M \to M$.“ Co to znamená? Znamená to to, že pro všechny uspořádané dvojice $(a, b) \in M \times M$ máme dobře definovaný výraz $a+b$. Tento výraz chápeme jako zobrazení dvou proměnných a podmínka $+ : M \times M \to M$ znamená, že každou dvojici $(a, b) \in M \times M$ zobrazí toto zobrazení zase zpět do množiny M. Říkáme, že M je **uzavřená vůči sčítání** $+$. Úplně stejně se můžeme dívat jako na násobení prvku množiny M reálným číslem α: je to zobrazení z $\mathbb{R} \times M$ opět do množiny M.

Kdyby se čtenář necítil ohledně této definice pevný v kramflecích, nechť si rozmyslí rovnosti v následujícím příkladě.

[24] Sami si rozmyslete, jaké všechny vlastnosti aritmetických operací s maticemi zde používáme.

Příklad 1.21. *Platí následující rovnosti:*

1. $\{4, -1\} + \{1, 2, 3\} = \{0, 1, 2, 5, 6, 7\}$
2. $\{1, -1\} + \{1, 2, 3\} = \{0, 1, 2, 3, 4\}$
3. $2\mathbb{Z}$ *je množina všech sudých celých čísel.*
4. $2\mathbb{Z} + 1$ *je množina všech lichých celých čísel.*
5. *Pro* $n \in \mathbb{Z}$ *je* $n\mathbb{Z}$ *množina všech celočíselných násobků* n*, tj.*
$$n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}.$$

Definici součtu množin budeme používat často i v následujících kapitolách[25], zde jej ale použijeme k přeformulování tvrzení *(iv)* a *(v)* z předchozí věty. Jelikož pro množinu matic $\mathbb{R}^{m,n}$ (a tedy i $\mathbb{R}^m$) máme dobře definované sčítání i násobení číslem, můžeme značení z předchozí definice bezstarostně používat.

Věta 1.22. *Nechť* $\tilde{\mathbb{x}}$ *je nějaké řešení soustavy* $\mathbb{A}\mathbb{x} = \mathbb{b}$*, potom pro tuto soustavu platí, že*
$$S = \tilde{\mathbb{x}} + S_0.$$

Když se nad tím trochu zamyslíme, zjistíme, že tato věta je skutečně ekvivalentní s tvrzeními *(iv)* a *(v)*: *(iv)* říká, že $S \subseteq \mathbb{x} + S_0$ a z *(v)* pak plyne, že $S \supseteq \mathbb{x} + S_0$. Dohromady tedy máme $S = \mathbb{x} + S_0$ a věta je dokázána.

Rovnost $S = \mathbb{x} + S_0$ může vypadat nevinně, ale pro naši snahu umět kompletně vyřešit libovolnou soustavu lineárních rovnic je klíčová, říká nám totiž, že **pokud chceme popsat celou množinu řešení, stačí umět najít jedno řešení a umět popsat množinu řešení přidružené homogenní soustavy**.

1.6 Gaussova eliminační metoda (GEM)

V této kapitole už jsme si vydatně o soustavách lineárních rovnic popovídali, takže je konečně čas si říci, jak hledat jejich řešení. Bohužel ještě nemáme veškerou výbavu k tomu, abychom tento úkol dotáhli úplně do konce. Přeci jen se ale mnoho důležitého o množině řešení zjistit naučíme. Konkrétně byste po přečtení této části měli být s to:

- Poznat, zda má soustava alespoň jedno řešení nebo nemá řešení žádné.
- Poznat, jestli má daná soustava právě jedno řešení nebo jich má nekonečně mnoho.
- V případě, že má soustava právě jedno řešení, toto řešení nalézt.
- V případě, že má soustava více než jedno řešení, nalézt jich nekonečně mnoho.

Co se zatím nedozvíte je to, jak popsat množinu řešení, když bude mít nekonečně prvků[26]. Popsat nekonečnou množinu je někdy záludný problém neb to samozřejmě

[25] Nota bene, je to velice obvyklé značení a často se používá bez dalšího komentáře, protože se předpokládá, že jej má laskavý čtenář v paži.

[26] Přesněji řečeno se to dozvíte, ale nebudete o tom vědět (tj. nebudeme schopní to dokázat).

nelze udělat prostým výčtem a musí se nějakým způsobem zachytit struktura této množiny. Někdy je to jednoduché, např. množinu sudých čísel popíšeme snadno:

$$\{2k \mid k \in \mathbb{Z}\},$$

jsou to prostě všechny celočíselné násobky dvou. A někdy je to zase extrémně složité, např. u množiny prvočísel. Tu popsat nějakým konečným způsobem, který by jasně říkal, jak všechna prvočísla vypadají, neumíme[27].

V případě řešení soustav lineárních rovnic si ukážeme, že množina S_0 vždy tvoří podprostor, tedy existuje konečná množina různých řešení (tzv. báze) taková, že všechna ostatní řešení získáme jejich lineární kombinací. Sami asi cítíte, že je trochu problém, že se tu oháníme pojmy, které Vám nic neříkají. O to, aby Vám něco říkali, se postaráme v další kapitole.

Horní stupňovitý tvar

V sekci 1.3 jsme viděli, že některé soustavy se dají vyřešit snadno, protože se dají přímočaře převést ze soustavy rovnic na řešení nezávislých lineárních rovnic s jednou proměnnou. Jako příklad jsme si uvedli soustavu (ta levá v (1.6)), kterou maticově můžeme zapsat

$$\left(\begin{array}{ccc|c} 3 & 2 & 1 & 6 \\ 0 & 2 & 1 & 3 \\ 0 & 0 & 1 & 1 \end{array}\right). \tag{1.11}$$

Vlastnost, která z této soustavy dělala snadno řešitelný problém, byla tato: Jedna z rovnic měla formu jednoduché lineární rovnice s jednou neznámou (konkrétně $z = 1$). Po jejím vyřešení a dosazení za tuto neznámou nám zbyly dvě rovnice pro dvě neznámé (zde jsou to x a y), jejichž tvar umožňoval opět jednu neznámou snadno spočítat. Toto navíc bylo možné opakovat, dokud jsme neohodnotili všechny proměnné.

Na soustavě (1.11) byla tato vlastnost snadno vidět, podobně snadno lze ale vyřešit třeba tuto soustavu:

$$\left(\begin{array}{ccc|c} 0 & 1 & 0 & 2 \\ 0 & 2 & -1 & 2 \\ 3 & 0 & 1 & 8 \end{array}\right). \tag{1.12}$$

Z první rovnice vykoukáme, že $y = 2$. Když za y dosadíme (prostřední sloupec vynásobíme dvěma, odečteme jej od sloupce pravých stran a následně jej vynulujeme – toto by se dalo popsat jako odečtení tohoto sloupce od obou stran soustavy), dostaneme:

$$\left(\begin{array}{ccc|c} 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -2 \\ 3 & 0 & 1 & 8 \end{array}\right), \tag{1.13}$$

což odpovídá soustavě dvou rovnic pro dvě neznámé x a z:

$$\left(\begin{array}{cc|c} 0 & -1 & -2 \\ 3 & 1 & 8 \end{array}\right). \tag{1.14}$$

[27] Kdybyste na něco přišli, můžete dostat buď hodně peněz, nebo taky záhadně zmizet, neb kvůli některým šifrám by z toho mohlo být docela mrzení.

V této soustavě máme další triviální rovnici $-z = -2$ s řešením $z = 2$. Po dosazení a dalším odečtení sloupce odpovídající proměnné z dostáváme

$$\left(\begin{array}{cc|c} 0 & 0 & 0 \\ 3 & 0 & 6 \end{array}\right),$$

což odpovídá rovnici $3x = 6$. Soustava má tedy jediné řešení a to $(2, 2, 2)$.

Když se podíváme (ne moc zkušeným okem) na soustavy (1.11) a (1.12), je jasné, že z tvaru té první je „snadná řešitelnost“ mnohem lépe vidět, neboť rovnici, která má snadné řešení, najdeme vždy dole a proměnnou této rovnice vždy vpravo. Jak uvidíme, na tento tvar se můžeme z (1.12) také dostat, aniž bychom měnili množinu řešení. V tomto konkrétním příkladu stačí napsat řádky v opačném pořadí (to jistě množinu řešení nemění) a prohodit druhý a třetí sloupec (to také množinu řešení nemění, neboť sčítání je komutativní[28]). Výsledkem je soustava

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

Nyní už by měl jen trochu zúčastněný čtenář být schopen vysvětlit[29], proč platí následující:

Pozorování 1.23. *Nechť pro matici soustavy* $\mathbb{A}\mathbb{x} = \mathbb{b}$ *platí následující:*

(i) $\mathbb{A} \in \mathbb{R}^{n,n}$ *(tj. je čtvercová),*

(ii) $\mathbb{A}_{ii} \neq 0$ *pro všechny* $i \in \{1, 2, \dots, n\}$ *(tj. diagonální prvky jsou nenulové),*

(iii) je-li $i > j$ *je* $\mathbb{A}_{ij} = 0$ *(tj. prvky pod diagonálou jsou nulové[30]),*

potom má soustava právě jedno řešení.

Jak již víme, soustavy nemusí mít vždy jediné řešení, mohou jich mít více (nekonečno) nebo nemusí mít žádné. Z toho je jasné, že ne všechny soustavy budeme s to převést na tvar popsaný v pozorování 1.23. Například soustava

$$\left(\begin{array}{ccc|c} 3 & 1 & 0 & 8 \\ 0 & -1 & 2 & 2 \\ 3 & 1 & 1 & 10 \\ 6 & 1 & 3 & 21 \end{array}\right)$$

řešení nemá, ale na první pohled to vidět není. Naopak u soustavy

$$\left(\begin{array}{ccc|c} 3 & 1 & 0 & 8 \\ 0 & -1 & 2 & 2 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{array}\right) \tag{1.15}$$

[28] Ha, další užitečná vlastnost!

[29] Pokud tomu nerozumíte, přečtete si tuto část ještě jednou. Tato „rada“ platí, i když už jste jí předtím četli. Stále platí, že bude hůř a tady není vůbec vhodné něco nechápat!

[30] Maticím splňující tento bod se říká **horní trojúhelníkové**.

to vidíme okamžitě, neb poslední řádek odpovídá neřešitelné rovnici[31] $0 = 1$.

Existuje tedy tvar soustavy, ze kterého je vidět, že má soustava právě jedno řešení a i tvar, který přímo křičí, že soustava řešení žádné nemá. Existuje tvar soustavy, ze kterého poznáme, že řešeních je více? Ano, koukněme třeba na následující soustavu tří rovnic o pěti neznámých $(x_1, x_2, x_3, x_4, x_5)$:

$$\left(\begin{array}{rrrrr|r} 3 & 1 & 0 & 2 & 0 & 7 \\ 0 & -1 & 2 & 2 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 2 \end{array}\right). \tag{1.16}$$

Najdeme si dvě různá řešení a s jejich pomocí dalších nekonečně mnoho řešení. Nejprve zkusme najít taková řešení, pro která je $x_3 = x_5 = 0$. To vlastně odpovídá tomu, že vynecháme třetí a pátý sloupec soustavy. Výsledkem je soustava pro tři neznámé (x_1, x_2, x_4)

$$\left(\begin{array}{rrr|r} 3 & 1 & 2 & 7 \\ 0 & -1 & 2 & 1 \\ 0 & 0 & 1 & 2 \end{array}\right),$$

která má, jak víme z pozorování 1.23, právě jedno řešení. Snadno spočítáme, že $x_4 = 2, x_2 = 3$ a $x_1 = 0$. Pro původní soustavu tedy dostáváme řešení $\mathbb{x} = (0, 3, 0, 2, 0)$. Když položíme $x_2 = x_4 = 0$, dostaneme podobně soustavu

$$\left(\begin{array}{rrr|r} 3 & 0 & 0 & 7 \\ 0 & 2 & 1 & 1 \\ 0 & 0 & 1 & 2 \end{array}\right),$$

která nám s použitím stejného postupu dá řešení $\mathbb{y} = (7/3, 0, -1/2, 0, 2)$.

Máme tedy dvě různá řešení soustavy (1.16) $\mathbb{x}, \mathbb{y} \in S$. Z bodu *(iii)* věty 1.19 víme, že vektor $\mathbb{z} = \mathbb{x} - \mathbb{y} = (-7/3, 3, 1/2, 2, -2)$ je řešením přidružené homogenní soustavy, neboli je prvkem S_0. Z bodu *(i)* téže věty víme, že vektor $\alpha\mathbb{z}$ je pro libovolné $\alpha \in \mathbb{R}$ také z S_0. Konečně podle bodu *(v)* platí, že pro libovolné $\alpha \in \mathbb{R}$ je vektor

$$\mathbb{x} + \alpha\mathbb{z} \in S$$

a my tak dostáváme *nekonečně mnoho* řešení!

Když se podíváme na soustavy (1.11), (1.15) a (1.16), u kterých jsme si ukázali, že je snadné je vyřešit, můžeme si všimnout jedné vlastnosti. Kdybychom v každém řádku nahradili nuly, které jsou nalevo od nejlevějšího nenulového prvku (v tomto řádku), nějakým kvádrem, dostaneme schody, po kterých budeme moci vystoupat

[31] Možná Vám připadá, že je to poněkud ulítlý příklad neřešitelné soustavy, ale není: každá neřešitelná soustava vede na takovouto zřejmou nepravdu. Ostatně když byste chtěli někoho přesvědčit, že rovnice $2x = 2(x + \pi)$ nemá řešení, také ukážete, že by muselo platit že $\pi = 0$.

až k prvnímu řádku. Ukažme[32] si to na soustavách (1.11), (1.15) a (1.16):

$$\left(\begin{array}{ccc|c} 3 & 2 & 1 & 6 \\ 0 & 2 & 1 & 3 \\ 0 & 0 & 1 & 1 \end{array}\right) \longrightarrow \left(\begin{array}{ccc|c} 3 & 2 & 1 & 6 \\ \blacksquare & 2 & 1 & 3 \\ \blacksquare & \blacksquare & 1 & 1 \end{array}\right)$$

$$\left(\begin{array}{ccc|c} 3 & 1 & 0 & 8 \\ 0 & -1 & 2 & 2 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{array}\right) \longrightarrow \left(\begin{array}{ccc|c} 3 & 1 & 0 & 8 \\ \blacksquare & -1 & 2 & 2 \\ \blacksquare & \blacksquare & 1 & 2 \\ \blacksquare & \blacksquare & \blacksquare & 1 \end{array}\right)$$

$$\left(\begin{array}{ccccc|c} 3 & 1 & 0 & 2 & 0 & 7 \\ 0 & -1 & 2 & 2 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 2 \end{array}\right) \longrightarrow \left(\begin{array}{ccccc|c} 3 & 1 & 0 & 2 & 0 & 7 \\ \blacksquare & -1 & 2 & 2 & 1 & 1 \\ \blacksquare & \blacksquare & \blacksquare & 1 & 1 & 2 \end{array}\right).$$

Tvaru, který tuto schodovitou vlastnost bude mít, říkáme **horní stupňovitý tvar**. Jelikož si tady jen tak nepovídáme, ale seriózně budujeme lineární algebru, musíme uvést řádnou a přesnou definici[33].

Poznámka 1.24. *Ve zbytku této kapitoly budeme předpokládat, že v matici soustavy nejsou sloupce obsahující samé nuly. Není to nikterak omezující předpoklad, pouze nám ulehčí (a zkrátí) práci. Např. soustava pro neznámé* (x, y, z, u)

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

je zjevně ekvivalentní soustavě pro neznámé (x, y, u)

$$\left(\begin{array}{ccc|c} 3 & 2 & 1 & 6 \\ 0 & 2 & 1 & 3 \\ 0 & 0 & 1 & 1 \end{array}\right).$$

Ta, jak víme, má jediné řešení $x = y = u = 1$). *Jelikož na proměnnou* z *v původní soustavě není kladena žádná podmínka (tj. nevyskytuje se v žádné rovnici), může mít jakoukoli hodnotu. Původní rovnice má tedy nekonečně mnoho řešení* $(1, 1, \alpha, 1)$, *kde* $\alpha \in \mathbb{R}$ *je libovolné.*

Definice 1.25. *Mějme soustavu lineárních rovnic* $\mathbb{A}\mathbb{x} = \mathbb{b}$, *kde* $\mathbb{A} \in \mathbb{R}^{m,n}$. *Řekneme, že soustava je v* ***horním stupňovitém tvaru****, jestliže existuje* $k \in \{1, \dots, m\}$ *tak, že řádky 1 až* k *rozšířené matice soustavy* $(\mathbb{A} \mid \mathbb{b})$ *jsou nenulové a řádky* $k+1$ *až* m *jsou nulové*[34] *a jestliže platí následující:*

Označme pro každé $i \in \{1, 2 \dots, k\}$ *index nejlevějšího nenulového prvku v itém řádku jako* j_i, *tj.*

$$j_i = \min\{\ell \in \{1, \dots, n+1\} \mid (\mathbb{A} \mid \mathbb{b})_{i\ell} \neq 0\}.$$

[32] Tady prosíme laskavého čtenáře o trochu fantazie, která mu z malých černých čtverečků udělá kvádry, které tvoří slibované schody.

[33] Pojem „schody“ nemá zřejmě rigorózní matematickou definici.

[34] Takto krkolomně říkáme, že případné nulové řádky matice musí být vyskládány dole.

Potom platí $1 = j_1 < j_2 < \cdots < j_k$.

Je-li soustava v horním stupňovitém tvaru, potom říkáme sloupcům s indexy $j_1, j_2, \ldots, j_k$ ***hlavní sloupce****, ostatním říkáme* ***vedlejší sloupce****.*

Poznámka 1.26. *Asi si říkáte: „Zlaté kvádry a schody, kdo se v tomhle má vyznat.“ Pokud přijdete na elegantnější přesnou definici horního stupňovitého tvaru, neváhejte napsat autorům, budou Vám vděční.*

Pro ujasnění značení uveďme následující příklad (používá značení z definice 1.25):

Příklad 1.27. *Pro soustavu* (1.11) *platí*

$$k = 3 \quad a \quad j_1 = 1 < j_2 = 2 < j_3 = 3.$$

Soustava je tedy dle definice v horním stupňovitém tvaru. Má tři hlavní sloupce (první, druhý a třetí sloupec) a jeden vedlejší (čtvrtý sloupec, neboli vektor pravých stran).

Pro soustavu (1.12) *platí*

$$k = 3 \quad a \quad j_1 = 2 = j_2 = 2 > j_3 = 1.$$

Tato soustava tedy není v horním stupňovitém tvaru.

Pro soustavu (1.15) *platí*

$$k = 4 \quad a \quad j_1 = 1 < j_2 = 2 < j_3 = 3 < j_4 = 4.$$

Tato soustava je v horním stupňovitém tvaru a všechny čtyři sloupce jsou hlavní.

Pro soustavu (1.16) *platí*

$$k = 3 \quad a \quad j_1 = 1 < j_2 = 2 < j_3 = 4.$$

Soustava je v horním stupňovitém tvaru. Má tři hlavní sloupce (první, druhý a čtvrtý sloupec) a tři vedlejší (třetí, pátý a šestý sloupec).

Na příkladech jsme si ukázali, že z horního stupňovitého tvaru umíme rozpoznat tři různé situace: soustava má právě jedno, resp. žádné, resp. více řešení. Tyto příklady byly v jistém smyslu univerzální, neboť platí následující věta.

Věta 1.28. *Mějme soustavu lineárních rovnic* $\mathbb{A}\mathbb{x} = \mathbb{b}$, *kde* $\mathbb{A} \in \mathbb{R}^{m,n}$. *Je-li tato soustava v horním stupňovitém tvaru, platí následující:*

(i) Je-li poslední sloupec matice $(\mathbb{A} \mid \mathbb{b})$ *hlavní, soustava nemá řešení.*

(ii) Je-li poslední sloupec matice $(\mathbb{A} \mid \mathbb{b})$ *jediný vedlejší sloupec, má soustava právě jedno řešení.*

(iii) Je-li poslední sloupec matice $(\mathbb{A} \mid \mathbb{b})$ *vedlejší a existuje-li ještě jiný vedlejší sloupec, má soustava více než jedno řešení.*

Jiný případ než tyto tři nastat nemůže.

Důkaz. Je jasné, že případy *(i)* – *(iii)* pokrývají všechny možnosti, které mohou nastat.

Tvrzení *(i)* je triviální, neboť z definice hlavního sloupce plyne, že rozšířená matice soustavy obsahuje řádek $\begin{pmatrix} 0 & 0 & \cdots & 0 \mid c \end{pmatrix}$, kde c je nenulové číslo. To ale odpovídá rovnici $0 = c$, která nemá řešení. Řešení tedy nemá ani soustava rovnic[35].

Předpoklad tvrzení *(ii)* vlastně znamená, že matice $\mathbb{A}$ splňuje předpoklady pozorování 1.23. Již nebudeme znovu vysvětlovat, že to znamená, že řešení soustavy je jednoznačně dané.

Zbývá ukázat, že platí *(iii)*. To ukážeme tak, že najdeme jedno řešení a pak nějaké nenulové řešení příslušné homogenní soustavy $\mathbb{A}\mathbb{x} = \theta$. Existence více než jednoho řešení pak již plyne z tvrzení *(v)* a *(i)* věty 1.19.

Jedno řešení získáme tak, že proměnné odpovídající vedlejším sloupcům v matici $\mathbb{A}$ (tj. vynecháváme z rozšířené matice sloupec pravých stran) položíme rovny nule. Je jasné, že po vynechání těchto vedlejších sloupců z matice $(\mathbb{A} \mid \mathbb{b})$, dostaneme matici v horním stupňovitém tvaru splňující předpoklad tvrzení *(ii)*. Takto vzniklá soustava má již jediné řešení, které doplníme do proměnných odpovídajícím hlavním sloupcům matice $(\mathbb{A} \mid \mathbb{b})$.

Označme vektor proměnných jako

$$\mathbb{x}^T = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix}.$$

Nenulové řešení soustavy $\mathbb{A}\mathbb{x} = \theta$ najdeme takto[36] Buď ℓ index nějakého vedlejšího sloupce. Označme matici, která vznikne z $\mathbb{A}$ vynecháním ℓtého sloupce, jako matici $\bar{\mathbb{A}} \in \mathbb{R}^{m,n-1}$. Podobně označme $\bar{\mathbb{x}}$ vektor, který vznikne z $\mathbb{x}$ vynecháním prvku x_ℓ. Soustava $\bar{\mathbb{A}}\bar{\mathbb{x}} = -\mathbb{A}_{:\ell}$ je jistě v horním stupňovitém tvaru, který splňuje buď předpoklad tvrzení *(ii)* nebo tvrzení *(iii)*. Pro takové soustavy ale již umíme najít řešení, označme jej $(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_{\ell-1}, \bar{x}_{\ell+1}, \ldots, \bar{x}_n)$. Z konstrukce tohoto řešení plyne, že $n$tice čísel $(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_{\ell-1}, 1, \bar{x}_{\ell+1}, \ldots, \bar{x}_n)$ je nenulové řešení původní homogenní soustavy $\mathbb{A}\mathbb{x} = \theta$. □

Konečně GEM

Zbývá ukázat, že každou soustavu lze převést na horní stupňovitý tvar. Využijeme k tomu úpravy (U1), (U2) a (U3) z části 1.4. Jelikož jsme ale pro soustavy začali používat maticový zápis, přeformulujeme si i tyto úpravy jako úpravy matice. Pro matici $\mathbb{A} \in \mathbb{R}^{m,n}$ s prvky a_{ij} definujeme[37] tyto operace:

(G1) Prohození dvou řádků.

---

[35] Vzpomeňme tvrzení *(ii)* v pozorování 1.4.

[36] Zkráceně bychom postup hledání tohoto řešení mohli popsat takto: vezměme nějaký (ne ten poslední) vedlejší sloupec v soustavě $\mathbb{A}\mathbb{x} = \theta$ a za příslušnou proměnnou dosaďme jedničku. Tento sloupec pak převeďme na pravou stranu (objeví se tam vynásobený číslem -1) a získáme tak nehomogenní soustavu. Ta nutně splňuje předpoklady *(ii)* nebo tvrzení *(iii)* a umíme ji tedy vyřešit. Nalezené řešení doplňme jedničkou za vynechanou proměnnou a získáme nenulové řešení původní homogenní soustavy.

[37] Písmeno G je od jména Gauss. Pojmenovávat různé věci po panu Gaussovi je v matematice takový folklór.

(G2) Vynásobení jednoho řádku matice nenulovým číslem, přesněji nahrazení řádku

$$\begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \end{pmatrix}$$

řádkem

$$\begin{pmatrix} \alpha a_{i1} & \alpha a_{i2} & \cdots & \alpha a_{in} \end{pmatrix},$$

pro nějaké $1 \leq i \leq m$ a $\alpha \in \mathbb{R} \setminus \{0\}$.

(G3) Přičtení libovolného násobku jednoho řádku k jinému, přesněji nahrazení řádku

$$\begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \end{pmatrix}$$

řádkem

$$\begin{pmatrix} (a_{i1} + \alpha a_{j1}) & (a_{i2} + \alpha a_{j2}) & \cdots & (a_{in} + \alpha a_{jn}) \end{pmatrix},$$

pro nějaká *různá* čísla $i, j \in \{1, 2, \ldots, m\}$ a $\alpha \in \mathbb{R}$.

Jelikož jsme vlastně pouze přeznačili úpravy U1 až U3, platí i analogická verze věty 1.5.

Věta 1.29. *Převedeme-li rozšířenou matici jedné soustavy na rozšířenou matici jiné pomocí jedné z úprav (G1), (G2) nebo (G3), mají obě soustavy stejnou množinu řešení.*

Nejprve si ukážeme, že matici každé soustavy umíme převést pomocí G1 až G3 do tvaru, kdy má v prvním sloupci nenulový prvek pouze v prvním řádku. Tento fakt pak využijeme ke konstrukci algoritmu, který převede libovolnou matici do horního stupňovitého tvaru. Postupovat budeme takto (upravujeme matici $\mathbb{A} \in \mathbb{R}^{m,n}$ s prvky a_{ij})

1. Pokud je $a_{11} = 0$, prohodíme 1. řádek s $i$tým řádkem, pro který je $a_{i1} \neq 0$. (úprava G1 a využití předpokladu o neexistenci nulového sloupce v matici soustavy)

2. Pro $j = 2, 3, \ldots, m$ přičteme k $j$tému řádku α násobek prvního řádku (úprava G3), kde α splňuje rovnici
$$a_{j1} + \alpha a_{11} = 0. \tag{1.17}$$

Naposledy si rozpitváme vlastnosti aritmetických operací s reálnými čísly: využili jsme toho, že rovnice (1.17) má v $\mathbb{R}$ vždy řešení, konkrétně $\alpha = -a_{j1}a_{11}^{-1}$. Jeho existence plyne z věty 1.1 a z její analogie pro sčítání, kterou také vyslovíme a dokážeme.

Věta 1.30. *Nechť $a, b \in \mathbb{R}$. Potom $x = -a + b$ je jediné reálné číslo splňující rovnici $a + x = b$.*

Důkaz. Nejprve ukážeme, že $x = -a + b$ je skutečně řešením rovnice $a + x = b$ a to prostě tak, že za x dosadíme a využijeme vlastností reálných čísel a jejich sčítání:

$$a + (-a + b) = (a + (-a)) + b = 0 + b = b.$$

První rovnítko jsme si mohli dovolit napsat díky tomu, že sčítání reálných čísel je asociativní. Druhé rovnítko je zase ospravedlněno tím, že každé reálné číslo a má inverzi (a značka $-a$ má tedy jasný význam) a že platí $a + (-a) = 0$. Poslední rovnítko stojí na jedinečné vlastnosti čísla 0: pro jakékoli reálné číslo c platí, že $0 + c = c$. Žádné jiné reálné číslo takovou vlastnost nemá.

Zbývá ukázat, že $x = -a+b$ je jediné řešení. Důkaz jednoznačnosti už nebudeme tolik pitvat, neboť se využívají stejné vlastnosti jako výše. Předpokládejme, že x' je také řešení dané rovnice. Potom platí:

$$\begin{aligned}
a + x' &= b && \text{// přičtěme inverz. prvek } -a \text{ zleva, existuje pro } \forall a\} \\
-a + (a + x') &= -a + b && \text{// přesuneme závorky díky asociativitě}\} \\
(-a + a) + x' &= -a + b && \text{// víme, že pro lib. } c \text{ je } -c + c = 0\} \\
0 + x' &= -a + b && \text{// pro libovolné } c \text{ je } 0 + c = c\} \\
x' &= -a + b.
\end{aligned}$$

Ukázali jsme, že má-li rovnice nějaké řešení, je toto řešení rovno $-a + b$ a důkaz je tak hotov. □

Proč to tady uvádíme, když je to triviální a navíc úplně stejné, jako v případě věty 1.1? Právě proto, abychom čtenáře upozornili na to, že je to stejné, neboť opět využíváme čtyři vlastnosti, které mají sčítání a násobení stejné: součet reálných čísel je reálné číslo, sčítání je asociativní, existuje speciální prvek nula, jehož přičtením se žádné číslo nemění a ke každému prvku existuje inverze (jen místo a^{-1} píšeme obvyklejší $-a$ a mluvíme o něm jako o prvku opačném k a).

Nyní tedy víme, že rovnice $a_{j1} + \alpha a_{11} = 0$ má řešení: víme totiž, že řešením rovnice $a_{j1} + y = 0$ je $y = -a_{ji}$ a řešením $\alpha a_{11} = -a_{ji}$ je $\alpha = -a_{j1}a_{11}^{-1}$.

A je to tady, můžeme si popsat **Gaussovu eliminační metodu**:

Algoritmus 1.31 (GEM). *Cíl algoritmu: Pro soustavu $\mathbb{A}\mathbb{x} = \mathbb{b}$, kde $\mathbb{A} \in \mathbb{R}^{m,n}$, hledáme takovou posloupnost úprav (G1) a (G3), která rozšířenou matici soustavy převede do horního stupňovitého tvaru.*

Postup: Položme $\mathbb{B} = (\mathbb{A} \mid \mathbb{b})$, $k = \ell = 1$. Dokud je $k \leq n$, provádíme následující:

1. *Pomocí úprav G1 a G3 a postupu popsaného výše vynulujte všechny prvky prvního sloupce mimo prvek na prvním řádku. Položte $k = k + 1$.*

2. *Platí-li $\mathbb{B}_{jk} = 0$ pro všechna $j = \ell + 1, \ell + 2, \ldots, m$, položte $k = k + 1$ a jděte do kroku 2.*

3. *Neplatí-li $\mathbb{B}_{jk} = 0$ pro všechna $j = \ell + 2, \ell + 3, \ldots, m$, zajistěte pomocí operací G1 a G3, aby to platilo (jak to udělat, je popsáno výše). Poté položte $k = k+1$, $\ell = \ell + 1$ a jděte do kroku 2.*

Pokud Vám tento popis není blízký[38], můžeme si algoritmus převyprávět pomocí dříve použitých schodů: V prvním kroku vytvoříme schod v prvním sloupci pomocí postupu popsaného výše v této části a přejdeme ke druhému sloupci, tj. $k = 2$. Druhý krok říká, že pokud máme v $k$tém sloupci schod stejně vysoký jako v předchozím

[38] Komu jinému by ale měl být blízký, než studentům FITu!

sloupci (tedy $m-\ell$), tak máme jít o sloupec doprava. Třetí krok pak říká, že pokud v $k$tém sloupci nemáme schod stejně vysoký, jako ve schodě předchozím, tak si vytvoříme schod o jeden stupínek nižší (výšky $m-\ell-1$) a jdu o sloupec doprava.

Pořadí úprav G1 a G3 v GEM není jednoznačně dané. Navíc můžeme použít pravidlo G2 a výpočty si tak případně zjednodušit. Při provádění GEM tedy máme poměrně velkou svobodu. Obecně platí, že se při provádění GEM vyplatí myslet pár tahů dopředu: při vhodném pořadí úprav si výpočet může významně ulehčit.

Uveďme si pro ilustraci běhu GEM následující příklad.

Příklad 1.32. *Rozhodněte, kolik má následující soustava pro neznámé $x_1, x_2, \ldots, x_5$ řešení:*

$$\left(\begin{array}{ccccc|c} 6 & 0 & 0 & 1 & 1 & 6 \\ 2 & 8 & 1 & 0 & 0 & -5 \\ 3 & 6 & 3 & 9 & 0 & -9 \end{array}\right)$$

Pomocí GEM upravujeme rozšířenou matici soustavy následovně. Kroku číslo 1 z algoritmu 1.31 odpovídají následující úpravy:

$$\left(\begin{array}{ccccc|c} 6 & 0 & 0 & 1 & 1 & 6 \\ 2 & 8 & 1 & 0 & 0 & -5 \\ 3 & 6 & 3 & 9 & 0 & -9 \end{array}\right) \xrightarrow[ř1 \leftrightarrow ř3]{G1} \left(\begin{array}{ccccc|c} 3 & 6 & 3 & 9 & 0 & -9 \\ 2 & 8 & 1 & 0 & 0 & -5 \\ 6 & 0 & 0 & 1 & 1 & 6 \end{array}\right) \xrightarrow[1/3 * ř1]{G2}$$
$$\left(\begin{array}{ccccc|c} 1 & 2 & 1 & 3 & 0 & -3 \\ 2 & 8 & 1 & 0 & 0 & -5 \\ 6 & 0 & 0 & 1 & 1 & 6 \end{array}\right) \xrightarrow[ř2 - 2*ř1]{G3} \left(\begin{array}{ccccc|c} 1 & 2 & 1 & 3 & 0 & -3 \\ 0 & 4 & -1 & -6 & 0 & 1 \\ 6 & 0 & 0 & 1 & 1 & 6 \end{array}\right) \xrightarrow[ř3 - 6*ř1]{G3}$$
$$\left(\begin{array}{ccccc|c} 1 & 2 & 1 & 3 & 0 & -3 \\ 0 & 4 & -1 & -6 & 0 & 1 \\ 0 & -12 & -6 & -17 & 1 & 24 \end{array}\right)$$

Nyní jsme se v algoritmu 1.31 dostali do kroku 2 (platí $k=2$ a $\ell=1$) Jelikož ale ve druhém sloupci nemáme na řádcích $\ell+1=2$ a $\ell+2=3$ nuly, jdeme do kroku 3. Zde opět není splněna podmínka, že ve druhém sloupci máme na třetím řádku nulu, musíme provést G3 a nulu si vyrobit: přičteme k třetímu řádku trojnásobek druhého (to zapisujeme jako $\xrightarrow[ř3+3*ř2]{G3}$) a dostaneme

$$\left(\begin{array}{ccccc|c} 1 & 2 & 1 & 3 & 0 & -3 \\ 0 & 4 & -1 & -6 & 0 & 1 \\ 0 & 0 & -9 & -35 & 1 & 27 \end{array}\right).$$

Tato matice je již v horním stupňovitém tvaru, a jelikož má tři vedlejší sloupce (4., 5. a 6.), má dle bodu (iii) ve větě 1.28 nekonečně mnoho řešení.

Pro radost si nějaká řešení najděme. Položme například $x_4 = x_5 = 0$. Dostaneme soustavu

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & -3 \\ 0 & 4 & -1 & 1 \\ 0 & 0 & -9 & 27 \end{array}\right),$$

která má jediné řešení $x_1 = 1, x_2 = -1/2, x_3 = -3$. Dostáváme tedy řešení, které můžeme zapsat ve tvaru pětice $(1, -1/2, -3, 0, 0)$.

Abychom nalezli nějaké řešení příslušné homogenní rovnice

$$\left(\begin{array}{ccccc|c} 1 & 2 & 1 & 3 & 0 & 0 \\ 0 & 4 & -1 & -6 & 0 & 0 \\ 0 & 0 & -9 & -35 & 1 & 0 \end{array}\right),$$

postupujme jako v důkazu bodu (iii) věty 1.28. Jednu proměnnou odpovídající vedlejšímu sloupci položíme rovnu nenulovému číslu (v důkazu je to 1, ale funguje to s libovolným nenulovým číslem) a ostatní položíme rovné nule. Když budeme trochu fundovaně koukat na tuto soustavu, vybereme si nastavení $x_4 = 0$ *a* $x_5 = 9$*. Odstraněním čtvrtého sloupce a převedením devítinásobku toho pátého na pravou stranu dostaneme soustavu*

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ 0 & 4 & -1 & 0 \\ 0 & 0 & -9 & -9 \end{array}\right),$$

která má jediné řešení $x_1 = -3/2, x_2 = 1/4, x_3 = 1$*. Dostáváme tedy nenulové řešení homogenní soustavy* $(-3/2, 1/4, 1, 0, -9)$*. Snadno již díky větě 1.19 dostaneme dalších nekonečně mnoho řešení.*

1.7 Těleso

Co jsme všechno potřebovali – shrnutí

V předchozích částech této kapitoly jsme mnohokrát zdůrazňovali, které vlastnosti reálných čísel a jejich násobení a sčítání potřebujeme, abychom dokázali to, co jsme zrovna dokazovali. Shrňme si teď tyto vlastnosti.
Co se násobení týče, potřebovali jsme tyto čtyři:

(i) množina reálných čísel je vůči násobení uzavřená, neboli $\forall a, b \in \mathbb{R} : ab \in \mathbb{R}$,

(ii) násobení je asociativní, neboli $\forall a, b, c \in \mathbb{R} : a(bc) = (ab)c$,

(iii) existuje reálné číslo 1 tak, že $\forall a \in \mathbb{R}$: $1a = a1 = a$,

(iv) každé nenulové číslo má inverzi, neboli $\forall a \in \mathbb{R} \setminus \{0\}$, $\exists a^{-1} \in \mathbb{R}$: $aa^{-1} = a^{-1}a = 1$.

Pro sčítání jsme potřebovali totéž:

(i) množina reálných čísel je vůči sčítání uzavřená, neboli $\forall a, b \in \mathbb{R} : a + b \in \mathbb{R}$,

(ii) sčítání je asociativní, neboli $\forall a, b, c \in \mathbb{R} : a + (b + c) = (a + b) + c$,

(iii) existuje reálné číslo 0 tak, že $\forall a \in \mathbb{R}$: $0 + a = a + 0 = a$,

(iv) každé číslo má opačný prvek, neboli $\forall a \in \mathbb{R}$, $\exists(-a) \in \mathbb{R}$: $a+(-a) = (-a)+a = 0$.

K tomu všemu jsme ještě potřebovali distributivní zákon (vytýkání ze závorky resp. roznásobení závorky):

$$\forall a, b, c \in \mathbb{R} : a(b + c) = ab + ac \wedge (b + c)a = ba + ca.$$

Nutně jsme nepotřebovali komutativitu násobení ani sčítání, ale dost nám při počítání usnadňovaly život.

Existuje mnoho dalších vlastností reálných čísel, která jsme nepotřebovali: vůbec jsme nepoužívali absolutní hodnotu, odmocňování (odmocnina kladného reálného čísla je zase reálné číslo), logaritmy, konvergenci (např. *úplnost* $\mathbb{R}$: každá konvergentní posloupnost má v $\mathbb{R}$ limitu) atd. Nabízí se tedy otázka, jestli bylo nutné uvažovat nutně množinu $\mathbb{R}$.

Zkusme nahradit množinu $\mathbb{R}$ množinou racionálních čísel $\mathbb{Q}$. Tato množina je opět uzavřená vůči sčítání i násobení a obě tyto operace jsou asociativní a platí pro ně distributivní zákon. Čísla 0 i 1 nám zůstávají, zbývá tedy otázka, zda v množině $\mathbb{Q}$ existuje inverzní resp. opačný prvek ke každému (nenulovému) racionálnímu číslu. Odpověď je samozřejmě ano: je-li $a \in \mathbb{Q}$, je i $-a \in \mathbb{Q}$. Podobně i a^{-1} je racionální, přidáme-li předpoklad, že a není 0. Celkově můžeme říci, že vše co fungovalo pro $\mathbb{R}$ platí i pro $\mathbb{Q}$: mohli bychom tedy zavést matice $\mathbb{Q}^{m,n}$, jejich násobení číslem z $\mathbb{Q}$, sčítání i násobení (matic vhodných typů). Můžeme každou matici upravit pomocí úprav G1, G2 (násobení číslem z $\mathbb{Q}$) a G3 na horní stupňovitý tvar a hledat řešení soustavy $\mathbb{A}\mathbb{x} = \mathbb{b}$, kde všechny matice a vektory mají prvky z $\mathbb{Q}$.

Motivovaný čtenář, nechť si rozmyslí, že úplně stejně bychom mohli zopakovat vše pro množinu $\mathbb{C}$ komplexních čísel a jejich sčítání a násobení. Co jiné[39] množiny, jako např. $\mathbb{Z}$ a $\mathbb{N}$? U obou bychom narazili: v $\mathbb{N}$ již na to, že v nich chybí nula a v $\mathbb{Z}$ nám zase chybí inverze a^{-1} (např. neexistuje celé číslo x tak, že $3x = 1$).

Příklad 1.33. *Uvažujme soustavu pro tři neznámé x, y, z:*

$$\left(\begin{array}{ccc|c} 2 & 4 & 6 & 0 \\ 3 & 6 & 11 & 1 \end{array}\right).$$

Jelikož číslo $3/2$ je v $\mathbb{R}, \mathbb{Q}$ i $\mathbb{C}$, můžeme v těchto množinách použít úpravu G3 a od druhého řádku odečíst první vynásobený $3/2$:

$$\left(\begin{array}{ccc|c} 2 & 4 & 6 & 0 \\ 0 & 0 & 2 & 1 \end{array}\right).$$

Tato matice je v horním stupňovitém tvaru, má dva vedlejší sloupce, z nichž jeden je sloupec odpovídající vektoru pravých stran. Podle věty 1.28 má více než jedno řešení. Když budeme chvilku počítat, zjistíme, že například $(-3/2, 0, 1/2)$ je řešení (v $\mathbb{Q}^3$, $\mathbb{R}^3$ i $\mathbb{C}^3$) a např. $(2, -1, 0)$ je řešení (také v $\mathbb{Q}^3$, $\mathbb{R}^3$ i $\mathbb{C}^3$) přidružené homogenní rovnice. Podle věty 1.22 pak máme, že

$$(-3/2, 0, 1/2) + \alpha(2, -1, 0)$$

je řešení[40] pro všechna α z $\mathbb{Q}$ resp. $\mathbb{R}$ resp. $\mathbb{C}$. Toto znamená, že např.

$$(-3/2, 0, 1/2) + 6/3(2, -1, 0)$$

[39] Po hříchu oblíbenější.

[40] Ve skutečnosti jsou to úplně všechna možná řešení, jak nám časem prozradí Frobeniova věta.

je řešení ve všech třech těchto množinách, ale např.

$$(-3/2, 0, 1/2) + \sqrt{2}(2, -1, 0)$$

je řešení jen v $\mathbb{R}$ *a* $\mathbb{C}$ *a*

$$(-3/2, 0, 1/2) + i(2, -1, 0)$$

jen v $\mathbb{C}$.

V množině celých čísel $\mathbb{Z}$ *bychom skončili už u úvodní úpravy G3, kde se násobilo číslem* $3/2 \notin \mathbb{Z}$. *Mohli bychom ale použít G1 a vynásobit první řádek 3 a druhý 2. Dostali bychom*

$$\left(\begin{array}{ccc|c} 6 & 12 & 18 & 0 \\ 6 & 12 & 22 & 2 \end{array}\right),$$

což lze pomocí G3 (přičtení $-1 \in \mathbb{Z}$ *násobku prvního řádku k druhému) upravit na*

$$\left(\begin{array}{ccc|c} 6 & 12 & 18 & 0 \\ 0 & 0 & 4 & 2 \end{array}\right).$$

I tato matice je v horním stupňovitém stavu a dle věty 1.28 by měla mít více než jedno řešení. Očividně tomu tak ale není: druhý řádek odpovídá rovnici $4z = 2$ *a ta v* $\mathbb{Z}$ *řešení nemá.*

Nechť si čtenář rozmyslí, že s trochou šikovnosti můžeme upravit matici na horní stupňovitý tvar pomocí G1, G2 a G3 i v množině $\mathbb{Z}$. *Nebudeme ale schopni využít větu 1.28, protože ta kvůli neexistenci (multiplikativních) inverzí*[41] *neplatí.*

Modulární aritmetika

Zatím jsme vyměňovali pouze množinu $\mathbb{R}$, my však půjdeme ještě dál: vyměníme i operace sčítání a násobení. Uděláme to tak šikovně, že si přeci jen vyrobíme z celých čísel strukturu, kde bude vše potřebné pro řešení soustav lineárních rovnic fungovat. Využijeme následující označení: pro libovolné celé $m \in \mathbb{Z}$ a přirozené $n \geq 2$ označíme

$$m \pmod{n}$$

zbytek po dělení čísla m číslem n. Zbytek bereme vždy z množiny[42] $\{0, 1, \ldots, n-1\}$. Např. platí

$$33 \pmod{7} = 5, \quad -3 \pmod{10} = 7, \quad 33 \pmod{11} = 0.$$

S pomocí tohoto značení můžeme zavést dvě nové binární operace[43]. První je **sčítání modulo** n, kde $n \geq 2$ je přirozené. Budeme jej značit $+_n$. Definované je následovně: pro libovolná celá čísla m a q definujeme

$$m +_n q := (m + q) \pmod{n}.$$

[41] A tedy i neplatnosti věty 1.1.

[42] Kdybychom chtěli být kujóni, mohli bychom říci, že zbytek po dělení 7 číslem 3 jsou 4, ale to by to dělení bylo takové nedotažené.

[43] Binární operaci na množině M prostě chápejte jako zobrazení z $M \times M$ do M.

Lapidárně řečeno, jedná se o klasické sečtení a poté aplikování $\pmod{n}$.

Analogicky definujeme **násobení modulo** n značené $\cdot_n$:

$$m \cdot_n q := (m \cdot q) \pmod{n}.$$

Pomocí těchto dvou operací budeme chtít sestrojit analogii množiny reálných čísel a jejich násobení a sčítání. K tomu budeme potřebovat mj. vědět, zda jsou sčítání a násobení modulo asociativní.

Lemma 1.34. *Sčítání a násobení celých čísel modulo n jsou asociativní a komutativní binární operace a platí pro ně distributivní zákon.*

Důkaz je technický a co do myšlenek triviální, a proto jej přeskočíme (resp. odsuneme do dodatku).

Zkusme nyní najít prvky, které by mohly hrát roli reálných čísel 0 a 1: hledáme tedy prvek $e \in \mathbb{Z}$ takový, že pro všechna $m \in \mathbb{Z}$ platí

$$e +_n m = m.$$

To je trochu problém, neboť výsledkem sčítání modulo n je vždy číslo z množiny $\{0, 1, \ldots, n-1\}$ a rovnost tak nemůže pro m mimo tuto množinu platit. Jak to vyřešíme? Omezíme se pouze na tuto množinu. Dokonce si pro ni zavedeme značku $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Nyní můžeme říci, že hledaný prvek je 0, neboť pro všechna $m \in \mathbb{Z}_n$ jistě platí, že

$$0 +_n m = m.$$

Role reálného čísla 1 také zůstane celému číslu 1, neboť pro všechna $m \in \mathbb{Z}_n$ jistě platí, že

$$1 \cdot_n m = m.$$

Zbývá nám najít opačné resp. inverzní prvky. S opačnými je to celkem jednoduché. Pro každé $m \in \mathbb{Z}_n$ hledáme nějaké $x \in \mathbb{Z}_n$ tak, že

$$m +_n x = 0.$$

Takové x ale snadno najdeme, je-li $m = 0$, je $x = 0$, jinak je $x = n - m$.

Příklad 1.35. *Uvažujme sčítání modulo* 13. *Potom skutečně platí, že* $0 +_{13} 0 = 0, 1 +_{13} 12 = 0, 2 +_{13} 11 = 0, 3 +_{13} 10 = 0, \ldots, 6 +_{13} 7 = 0$ *(dále je to díky komutativitě* $+_{13}$ *jasné).*

Zbývají inverzní prvky: pro každé $m \in \mathbb{Z}_n$ bychom chtěli najít x tak, že

$$m \cdot_n x = 1.$$

To jistě nepůjde pro $m = 0$ a budeme se muset omezit na $\mathbb{Z}_n \setminus \{0\}$, to nám ale nevadí, neboť to jsme museli udělat i v reálných číslech. Stačí ale toto omezení? Zkusme hledat inverzní prvek k číslu 2 při násobení modulo 6. Platí následující:

$$2 \cdot_6 1 = 2, 2 \cdot_6 2 = 4, 2 \cdot_6 3 = 0, 2 \cdot_6 4 = 2, 2 \cdot_6 5 = 4.$$

Dvojka tedy inverzi nemá. Můžeme si ale například všimnout, že $5 \cdot_6 5 = 1$, tedy že číslo 5 inverzi má. Důvod, proč 2 inverzi nemá a 5 má, je ten, že pětka je s 6 nesoudělná a dvojka nikoli[44].

Lemma 1.36. *Nechť $n \geq 2$ je přirozené číslo. Pro $m \in \mathbb{Z}_n \setminus \{0\}$ má rovnice*

$$m \cdot_n x = 1$$

řešení $x \in \mathbb{Z}_n$, právě když jsou m a n nesoudělná.

Lemma opět dokazovat nebudeme a necháme si to do kurzu BI-ZDM[45]. Důkaz opět není složitý, ale není ani moc „lineárně algebraický“.

Co jsme se tedy dozvěděli: mají-li mít všechny prvky $\mathbb{Z}_n \setminus \{0\}$ inverzi, musí být všechny nesoudělné s n. Taková situace ale nastává pouze tehdy, je-li n prvočíslo!

Grupa a těleso

Mohli bychom teď skončit s tím, že vše co funguje v $\mathbb{R}$ s klasickým sčítáním a násobením funguje i v $\mathbb{Z}_p$, kde p je prvočíslo a kde se sčítá a násobí modulo p. My však naši snahu dotáhneme ještě dál.

Co tím myslíme, si ukážeme opět na větě 1.1, resp. její obdobě pro sčítání 1.30. Ještě jednou si ji dokážeme[46]. Tentokrát ale nebudeme uvažovat konkrétní množinu (jako např. $\mathbb{R}, \mathbb{Q}, \mathbb{Z}_p, \ldots$) a konkrétní operaci (jako např. $+, \cdot, +_p, \cdot_p, \ldots$). My už tušíme, že věta platí pro libovolnou množinu a binární operaci, pokud splňují požadované vlastnosti. Taková struktura má ale v matematice jméno a je to velmi často používané jméno!

Definice 1.37. *Nechť M je neprázdná množina a $\circ : M \times M \to M$ binární operace. Platí-li*

(i) $\forall a, b, c \in M : a \circ (b \circ c) = (a \circ b) \circ c$ *(asociativní zákon),*

(ii) existuje $e \in M$ tak, že $\forall a \in M : a \circ e = e \circ a = a$ (existence ***neutrálního prvku****),*

(iii) $\forall a \in M, \exists a^{-1} : a \circ a^{-1} = a^{-1} \circ a = e$ *(existence* ***inverzních prvků****),*

říkáme, že uspořádaná dvojice $G = (M, \circ)$ je ***grupa****.*

Je-li navíc $\circ$ komutativní, tj. $\forall a, b \in M : a \circ b = b \circ a$, mluvíme o ***Abelovské grupě****.*

Poznámka 1.38. *Značení $\circ$ pro binární operaci jsme použili, abychom abstrahovali od obvyklých značek pro binární operace $+$ a $\cdot$ a zdůraznili tak, že se jedná o libovolnou binární operaci. Ostatně, prvky uvažované grupy vůbec nemusí být čísla. Značení $(M, +)$ a $(M, \cdot)$ pro grupy se ale také běžně používá a my jej budeme též*

[44] Dvě celá čísla jsou nesoudělná, je-li jejich největší společný dělitel číslo 1. Např. prvočíslo p je nesoudělné se všemi čísly $1, 2, \ldots, p-1$. Nula naopak není nesoudělná s žádným číslem větším než jedna, neboť každé číslo dělí nulu.

[45] Základy diskrétní matematiky, zimní semestr druhého ročníku.

[46] Slibujeme, že už je to opravdu naposledy.

používat, jelikož zavádět novou značku pro klasické sčítání je čistá šikana studentů. Použije-li se ale značka $+$, značíme inverzní prvek spíše $-a$ a říkáme mu opačný, neutrálnímu prvku se pak někdy říká nulový. Podobně při značení $\cdot$ se neutrálnímu prvku někdy říká jednotkový prvek. Místo $a + (-b)$ obvykle píšeme $a - b$.

Věta 1.39. *Nechť $(M, \circ)$ je grupa a $a, b \in M$. Potom $x = a^{-1} \circ b$ je jediný prvek M splňující rovnici $a \circ x = b$.*

Důkaz. Nejprve ukážeme, že $x = a^{-1} \circ b$ je skutečně řešením rovnice $a \circ x = b$ a to prostě tak, že za x dosadíme, a využijeme vlastností grupy:

$$a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b.$$

První rovnítko jsme si mohli dovolit napsat díky tomu, že $\circ$ je *asociativní*. Druhé rovnítko je ospravedlněno tím, že každé $a \in M$ má inverzní prvek, pro který platí $a \circ a^{-1} = e$. Poslední rovnítko stojí na vlastnosti neutrálního prvku.

Zbývá ukázat, že $x = a^{-1} \circ b$ je jediné řešení. Předpokládejme, že x' je také řešení dané rovnice. Potom platí:

$$\begin{aligned}
a \circ x' &= b && \text{// vynásob inverzním prvkem } a^{-1} \text{ zleva}\\
a^{-1} \circ (a \circ x') &= a^{-1} \circ b && \text{// přesuň závorky (asociativita)}\\
(a^{-1} \circ a) \circ x' &= a^{-1} \circ b && \text{// pro každé } a \text{ je } a^{-1} \circ a = e\\
e \circ x' &= a^{-1} \circ b && \text{// pro každé } c \text{ je } 1 \circ c = c\\
x' &= a^{-1} \circ b.
\end{aligned}$$

Ukázali jsme, že má-li rovnice $a \circ x = b$ nějaké řešení, je tímto řešením právě prvek $a^{-1} \circ b \in M$. Důkaz je tak hotov. □

Nyní bychom mohli věty 1.1 a 1.30 zahodit, neboť jsou okamžitým důsledkem předchozí věty a faktu, že $(\mathbb{R}, +)$ a $(\mathbb{R} \setminus \{0\}, \cdot)$ jsou grupy[47].

Věta 1.39 platí pro jakoukoli grupu, tedy i pro ty, se kterými jsme se doposud setkali. Pro přehlednost je shrňme v následujícím pozorování.

Pozorování 1.40. *Následující uspořádané dvojice (množina, binární operace) tvoří grupu:*

$$(\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{C}, +), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot), (\mathbb{Z}_n, +_n), (\mathbb{Z}_p \setminus \{0\}, \cdot_p),$$

kde $n \geq 2$ je přirozené číslo a p je prvočíslo.

Ve všech těchto množinách má tedy rovnice $a \circ x = b$, kde $\circ$ je příslušná binární operace, jednoznačné řešení!

Nám ale nestačí, že umíme najít abstraktní strukturu, kde umíme řešit lineární rovnici o jedné neznámé. My bychom chtěli umět řešit soustavy lineárních rovnic o libovolném počtu neznámých, stejně jako jsme si to ukázali pro reálná čísla. K tomu už nám ale moc nezbývá! Chybí nám možnost používat jak sčítání tak násobení najednou (v grupě máme vždy jen jednu binární operaci) a navíc distributivní zákon. I pro takovou strukturu máme v matematice jméno:

[47] Tuhle větu si pro dobro veškerenstva rozmyslete!!

Definice 1.41. *Nechť M je neprázdná množina a $+ : M \times M \to M$, $\cdot : M \times M \to M$ dvě binární operace. Platí-li, že*

(i) *$(M, +)$ je Abelovská grupa (neutrální prvek značíme 0 a nazýváme **nulový prvkem**),*

(ii) *$(M \setminus \{0\}, \cdot)$ je grupa (neutrální prvek značíme 1 a nazýváme **jednotkový prvek**),*

(iii) *platí levý a pravý[48] distributivní zákon, tj.*

$$\forall a, b, c \in M : a(b + c) = ab + ac \wedge (b + c)a = ba + ca,$$

*nazýváme uspořádanou trojici $T = (M, +, \cdot)$ **tělesem**.*

*Je-li navíc $(M \setminus \{0\}, \cdot)$ Abelovská grupa, je T **komutativní těleso**.*

Poznámka 1.42. *V celém následujícím textu budeme z praktických důvodů uvažovat pouze komutativní tělesa, ať už to bude explicitně zdůrazněno nebo ne.*

Z definice tělesa snadno plynou některé další vlastnosti. Například, pro každé $a \in T$ platí $0a = 0$. Je totiž $0a = (0 + 0)a = 0a + 0a$, přitom prvek $u \in T$ splňující $u = u + u$ splňuje též $0 = u - u = (u + u) - u = u + (u - u) = u + 0 = u$.[49]

Pokud jste četli pozorně, nemělo by Vás překvapit to, co se tvrdí v následující větě.

Věta 1.43. *Množiny $\mathbb{R}, \mathbb{Q}$ a $\mathbb{C}$ spolu s klasickým sčítáním a násobením tvoří tělesa. Podobně $(\mathbb{Z}_p, +_p, \cdot_p)$ je pro prvočíslo p těleso.*

Poznámka 1.44. *Těleso budeme obvykle značit T. Budeme-li mluvit ale například o tělese $(\mathbb{R}, +, \cdot)$, budeme-jej zkráceně značit $\mathbb{R}$, tak jak jsme vlastně zvyklí. Podobně o $\mathbb{Z}_p$ budeme říkat, že je to těleso a implicitně budeme předpokládat, že operacemi jsou sčítání a násobení modulo p.*

Nyní můžeme slavnostně završit celou kapitolu následujícím tvrzením:

> Vše co jsme si ukázali pro těleso $\mathbb{R}$ platí i pro libovolné jiné těleso. Máme tedy vlastně zavedeny matice $T^{n,m}$ s prvky z tělesa T, rovnici $\mathbb{A}\mathbb{x} = \mathbb{b}$, kde $\mathbb{A}$, $\mathbb{x}$ a $\mathbb{b}$ jsou matice resp. vektory příslušných rozměrů, říkáme soustava lineárních rovnic, i když T není $\mathbb{R}$. Víme, že pomocí úprav G1, G2 a G3 umíme libovolnou matici soustavy upravit na horní stupňovitý tvar a z něho rozhodnout, zda má jedno řešení, více než jedno řešení[50], příp. nemá řešení žádné.

[48] Pokud není operace $\cdot$ komutativní, mohlo by se stát, že platí distributivní zákon pouze při násobení závorky zleva. Proto v definici tělesa požadujeme obojí. Naštěstí ale tělesa, se kterými budeme pracovat v tomto kurzu, budou vždy komutativní.

[49] Alternativně lze využít již dokázané vlastnosti o grupě $(T, +)$, a to, že každá rovnice $a + x = b$ ($a, b \in T$) má právě jedno řešení $x \in T$. Uvažujeme-li rovnici $0a + x = 0a$, ta má jistě za své řešení $x = 0$, ale současně také $x = 0a$, neboť $0a + 0a = (0 + 0)a = 0a$. Tedy $0a = 0$.

[50] Zde by si šťouravý čtenář mohl vzpomenout na tvrzení, které platilo v tělese $\mathbb{R}$ ale neplatí v tělesech $\mathbb{Z}_p$. Místy jsme totiž tvrdili, že soustava může mít nekonečně řešení. Je-li ale $\mathbb{x} \in \mathbb{Z}_p^n$, tj. vektor neznámých má prvky v konečném tělese, těžko může mít soustava nekonečně mnoho řešení. Vždyť i kdyby bylo řešení každé $\mathbb{x} \in \mathbb{Z}_p^n$, máme stále pouze p^n různých řešení.

Jelikož práce s konečnými tělesy může být pro některé čtenáře nezvyklá, uveďme si několik ukázkových výpočtů.

Příklad 1.45. *TBA*

1.8 Dodatky

Zde si uvedeme pár zajímavostí, které doplňují tuto kapitolu. Aby si čtenář mohl čtení těchto zajímavostí užít, oznamujeme, že se nejedná o látku, která by se mohla objevit v jakékoli písemce.

Konečná tělesa: vlastnosti

Zde si **výhledově** uvedeme důkaz, že sčítání a násobení modulo jsou asociativní operace a také si ukážeme, jak se hledají inverzní prvky pro násobení modulo n a proč existují jen pro čísla nesoudělná s modulem.

Konečná tělesa: aplikace

Konečná tělesa jsou pro informatiky zajímavá zejména tím, že se v nich kóduje a šifruje. O kódování budeme mluvit později, o šifrování se stručně zmíníme (opět **výhledově**) zde. Více o šifrování uslyšíte v kurzu BI-BEZ[51].

Konečná tělesa neprvočíselného řádu

Tělesa $\mathbb{Z}_p$ nejsou jediná konečná tělesa. To není moc překvapivé, vždyť těleso je hodně obecná struktura vymezená jen několika jednoduchými vlastnostmi. Přesto ale nemůžeme tělesa úplně jednoduše sypat z rukávu: např. lze ukázat, že neexistuje těleso, které by mělo 10 prvků. Platí totiž, že je-li T těleso s konečným počtem prvků, je tento počet mocnina prvočísla (tj. konečná tělesa mají p^k prvků, kde p je prvočíslo a k je přirozené číslo). Tělesa s počtem prvků p jsme si ukázali, jsou to tělesa $\mathbb{Z}_p$. Zde si (**výhledově**) naznačíme, jak se konstruují tělesa s neprvočíselným počtem prvků.

[51] Bezpečnost, letní semestr druhého ročníku.

Kapitola 2

Základní pojmy lineární algebry

V předchozí kapitole už jsme se setkali s pojmem *vektor*, jednalo se ovšem o poměrně přízemní[1] pojem – vektory byly nazývány jakékoli $n$tice reálných čísel.

Geometrickou představu takových $n$tic dobře známe z dřívějších fází vzdělávacího procesu. Je-li[2] $n \leq 3$, umíme si $n$tici reálných čísel poměrně snadno představit jako bod v $n$rozměrném prostoru (nebo také $n$dimenzionálním – oba pojmy prozatím chápeme pouze intuitivně![3]) o daných souřadnicích (v pravoúhlém systému os $x, y, z, \dots$), případně jako orientovanou úsečku (šipku), která začíná v počátku soustavy souřadnic a končí v bodě o daných souřadnicích.

Aniž bychom se nad tím kdovíjak zamýšleli, s takovými vektory umíme jednoduše pracovat – jak si dále ukážeme, umíme je sčítat mezi sebou a násobit reálným číslem. Pro tyto operace platí v jistém smyslu pěkné vlastnosti, víme například, že nezáleží na pořadí, v jakém vektory sčítáme, že vynásobením libovolného vektoru číslem 1 se tento vektor nezmění, a tak dále. Tyto vlastnosti, platné pro šipky v rovině či prostoru (dvojice či trojice reálných čísel) spolu s tělesem reálných čísel a operacemi „sčítání šipek“ a „násobení šipek čísly“, zobecníme a nazveme je axiomy.

Zvolíme-li si pak libovolně číselné těleso a nějakou množinu prvků spolu se dvěma operacemi, které formálně nazveme sčítání (prvku s prvkem) a násobení (prvku číslem z tělesa), tak ať už těmito prvky bude cokoli[4], stačí, aby byly splněny ony axiomy, a tyto prvky budeme moci hrdě nazvat vektory (a pohodlně s nimi pracovat).

2.1 Co si z této kapitoly odneseme

1. Ze středoškolských znalostí si připomeneme pojem vektorů jako orientovaných úseček a početní operace s nimi.

2. Zavedeme si pojem *vektorový prostor* ve vší obecnosti, pomocí takzvaných *axiomů* vektorového prostoru. Přitom pochopíme, že všechny dosavadní geometrické představy o pojmu vektor byly jen velice speciální případy.

[1] Pojem přízemní chápejme jako „nedostatečně abstraktní“, případně „příliš snadno představitelný v reálném životě“.

[2] Pohádkové číslo 3 je hranicí pro lidskou představivost, nikoli však pro lineární algebru.

[3] Tohoto luxusu si užijme, dokud můžeme. Jakmile k jakémukoli pojmu uvedeme precizní definici, stává se jeho „intuitivní popis“ silně nežádoucím, především pak u zkoušky!

[4] Čísla, $n$tice čísel, matice, posloupnosti, polynomy, reálné funkce, cokoli nás napadne. . .

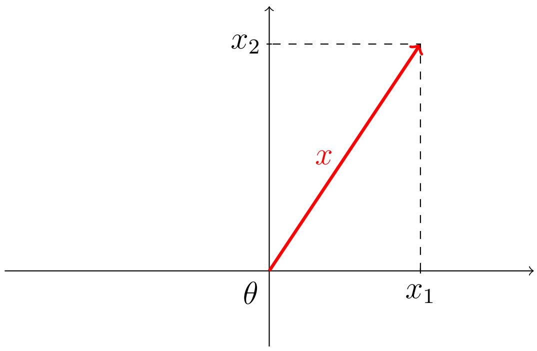
3. Smíříme se s tím, že postup „od obecného ke konkrétnímu“ je mnohem výhodnější, než ten opačný[5]. Namísto dokazování různých pravd a vlastností v každém konkrétním vektorovém prostoru zvlášť je totiž stačí dokázat jen jednou – pro libovolný vektorový prostor, pouze s využitím axiomů a z nich odvozených tvrzení.

4. Zavedeme si pojem podprostor a pomocí dalších pojmů, jako například lineární (ne)závislost, postupně dojdeme k přesnému zavedení pojmu *báze* vektorového prostoru a jeho *dimenze*.

2.2 Prostor šipek v rovině

Uvažujme těleso $\mathbb{R}$ všech reálných čísel. Prvky $\mathbb{R}^2$ jsou uspořádané reálné dvojice, které umíme jednak sčítat mezi sebou, jednak násobit reálným číslem – obě operace definujeme tzv. po složkách, viz definice 1.7. Abychom tyto operace odlišili od klasického sčítání a násobení reálných čísel, dočasně je označíme jako $\oplus$, resp. $\odot$.

Geometricky si lze prvky $\mathbb{R}^2$ představovat jako body roviny $x = (x_1, x_2)$. Pro geometrickou ilustraci operací $\oplus$ a $\odot$ je názorné spojit bod (x_1, x_2) s pevně zvoleným počátkem $\theta = (0, 0)$ a uvažovat o prvcích $\mathbb{R}^2$ jako o tzv. **orientovaných úsečkách**:

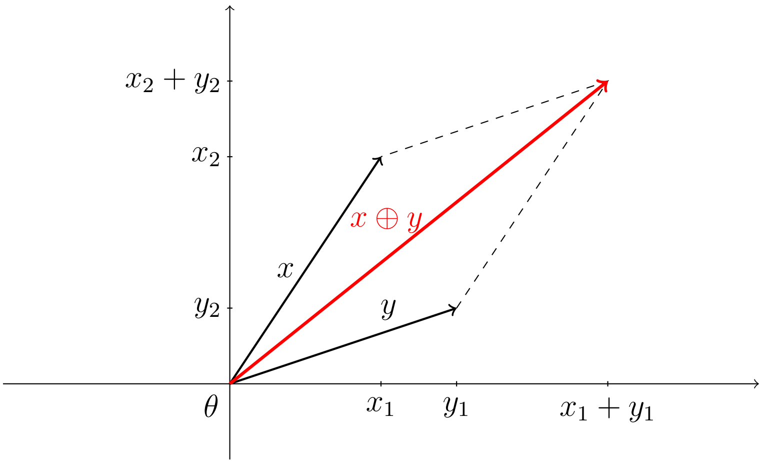


Sčítání prvků $\mathbb{R}^2$ po složkách,

$$x \oplus y = (x_1, x_2) \oplus (y_1, y_2) := (x_1 + y_1, x_2 + y_2),$$

pak odpovídá přirozenému skládání orientovaných úseček:

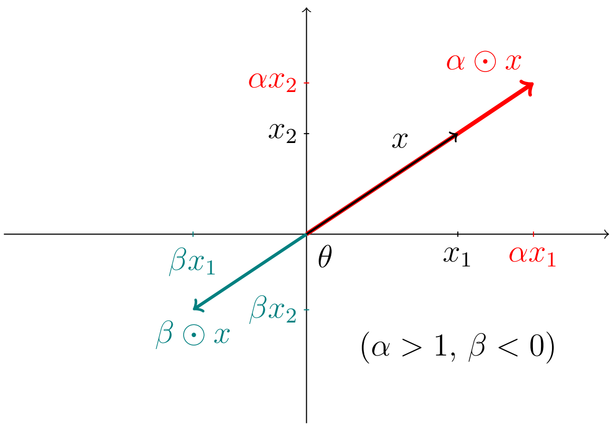
[5]Nebo se o to budeme alespoň usilovně snažit. Typický student je často navyklý obrácenému postupu a tvrdohlavě začíná pitváním se v příliš konkrétních příkladech – z těch se pak pokouší vyvozovat obecná tvrzení. To sice může pomoci v těžkých začátcích a i my v textu obvykle začínáme příklady, nicméně pro hladký průchod kurzem Lineární algebry je jistá schopnost abstrakce nezbytná!



Podobně, násobení číslem orientovanou úsečku pouze prodlužuje nebo zkracuje,

$$\alpha \odot x = \alpha \odot (x_1, x_2) := (\alpha x_1, \alpha x_2).$$

Směr orientované úsečky se buďto vůbec nemění (pro $\alpha > 0$), nebo se celá orientovaná úsečka „překlopí“ podle počátku θ na opačnou polopřímku (pro $\alpha < 0$)[6]:



Laskavý čtenář si doma jistě sám ověří (ať už geometrickou „šipkovou“ úvahou, nebo čistě početně s využitím definice sčítání a násobení pro orientované úsečky[7]), že ve světě orientovaných úseček v rovině, vybudovaném nad tělesem reálných čísel $\mathbb{R}$ a vybaveném operacemi $\oplus, \odot$, platí některé očividné pravdy, shrnuté v následujícím pozorování, a to velmi neformálním a ostudně nematematickým jazykem[8].

Pozorování 2.1. *Uvažujme prvky $\mathbb{R}^2$ (nazvěme je „vektory“) s operacemi $\oplus$ (sčítání) a $\odot$ (násobení reálným číslem) definovanými po složkách. Množina vektorů v $\mathbb{R}^2$ je **uzavřená** na obě operace $\oplus, \odot$[9] a dále splňuje následující vlastnosti (uvažovaná reálná čísla a vektory mohou být libovolné):*

[6] Chybějící případ $\alpha = 0$ je triviální, násobením nulou dostaneme vždy úsečku nulové délky.

[7] Tento způsob je pro nás samozřejmě atraktivnější. Navíc je to užitečný trénink pro budoucí dokazování všelijakých matematických tvrzení.

[8] Takové nepřesné vyjadřování sami doma nezkoušejte, my už to taky víckrát neuděláme!

[9] Lidově řečeno: sečteme-li dva vektory, dostaneme opět vektor v $\mathbb{R}^2$ a, podobně, vynásobíme-li vektor číslem, výsledkem bude opět vektor v $\mathbb{R}^2$.

1. *Nezáleží na pořadí, v jakém vektory sčítáme.*

2. *Sčítáme-li tři vektory, můžeme nejprve sečíst první dva a k výsledku přičíst třetí, nebo obráceně (první vektor přičíst k už provedenému součtu dalších dvou) a výsledek se nezmění.*

3. *Vynásobíme-li vektor jedním číslem a poté druhým, dostaneme totéž, jako bychom ho násobili najednou součinem těchto čísel.*

4. *Vynásobíme-li dva vektory stejným číslem a výsledky sečteme, dostaneme totéž, jako bychom vektory nejprve sečetli a až pak tímto číslem vynásobili.*

5. *Vynásobíme-li stejný vektor zvlášť dvěma čísly a tyto dva výsledky sečteme, dostaneme totéž, jako bychom tento vektor rovnou vynásobili součtem obou čísel.*

6. *Vynásobíme-li libovolný vektor jedničkou, nezmění se.*

7. *V rovině existuje vektor, který můžeme dostat vynásobením libovolného vektoru nulou, je to tzv. nulový vektor θ („šipka začínající a končící v počátku“).*

2.3 Vektorový prostor

Předpokládejme, že nás zajímá pouze prostor $\mathbb{R}^2$ orientovaných úseček v rovině zavedený v části 2.2. Mít velmi malé cíle, mohli bychom celou teorii lineární algebry vybudovat pouze pro $\mathbb{R}^2$ – odvodili bychom si, jak popsat podprostory v rovině, jak hledat jejich báze, jak řešit soustavy nejvýše dvou rovnic o nejvýše dvou proměnných, jak popisovat lineární zobrazení v rovině a pracovat s nimi, jak řešit geometrické úlohy v rovině, a mnoho dalších věcí.

Jednoho krásného dne nám ale začne být v rovině příliš těsno – z $\mathbb{R}^2$ přejdeme do $\mathbb{R}^3$ a začneme pracovat s trojicemi reálných čísel, které lze také sčítat mezi sebou a násobit reálným číslem (po složkách). V tom případě si opět můžeme uvědomit několik základních vlastností, v duchu pozorování 2.1, a pokračovat krok za krokem v budování nové teorie – zjistíme, že v podstatě všechno funguje úplně „stejně“[10] v $\mathbb{R}^3$ jako v $\mathbb{R}^2$

Přirozeně dojdeme k potřebě pracovat „ve více dimenzích“, například u řešení soustav lineárních rovnic pro více než tři proměnné – začneme pracovat se čtveřicemi, péticemi,... obecně s $n$ticemi reálných čísel ($n \geq 1$) a opět vše odvodíme znovu, pro množinu $\mathbb{R}^n$, s ne příliš odlišným výsledkem[11].

V různých situacích můžeme dojít k potřebě pracovat s prvky všelijakých množin jako s *vektory v nějakém prostoru*, může jít o matice, nekonečné posloupnosti, polynomy, spojité funkce i o mnohem roztodivnější objekty. Můžeme se setkat s potřebou pracovat s jinými než reálnými $n$ticemi, například nad tělesem $\mathbb{Q}$, $\mathbb{C}$, nebo $\mathbb{Z}_p$ v případě modulární aritmetiky (viz část 1.7), dokonce se můžeme setkat i s

[10] Nebo alespoň analogicky...

[11] Oblíbenou ilustrací obráceného principu je pak otázka, jakým způsobem si matematik představuje čtyřrozměrný prostor. Jednoduše, představí si prostor $n$rozměrný a pak zvolí $n = 4$.

„exoticky“ definovanými operacemi $\oplus$, $\odot$. Pokud nepřekonáme propast mezi konkrétním a obecným, budeme vždy (pro každou volbu tělesa, množiny vektorů a operací) nuceni budovat od základů celou potřebnou teorii znovu! To pochopitelně není ta správná cesta…

Hlavní pointa celé teorie, kterou v průběhu kurzu BI-LIN společně vybudujeme, pak spočívá v tom, že vlastně příliš nezáleží na tom, které konkrétní těleso („množinu používaných čísel“, viz definice 1.41) zvolíme, jaké objekty nazýváme vektory a jak přesně definujeme operace $\oplus$, $\odot$. Jediné na čem záleží je, jestli jsou splněny konkrétní základní vlastnosti – přesně ty, které jsme v pozorování 2.1 popsali pro šipky v rovině – ty nazveme axiomy. Čistě z těchto axiomů pak odvodíme veškerou teorii, která pak bude univerzálně platit úplně stejně pro každou strukturu, která tyto axiomy splňuje! Takové struktury budeme nazývat *vektorové prostory*:

Definice 2.2. *Nechť T je libovolné komutativní těleso, jeho neutrální prvky vůči operacím sčítání resp. násobení označme 0, resp. 1. Nechť je dále dána neprázdná množina V a dvě zobrazení*

$$\oplus : V \times V \to V, \qquad \odot : T \times V \to V\,.$$

*Řekneme, že V je **vektorový prostor nad tělesem** T s vektorovými operacemi $\oplus$ a $\odot$, právě když platí následující **axiomy vektorového prostoru**:*

1. $\forall a, b \in V : a \oplus b = b \oplus a,$
2. $\forall a, b, c \in V : (a \oplus b) \oplus c = a \oplus (b \oplus c),$
3. $\forall \alpha, \beta \in T, \forall a \in V : \alpha \odot (\beta \odot a) = (\alpha\beta) \odot a,$
4. $\forall \alpha \in T, \forall a, b \in V : \alpha \odot (a \oplus b) = (\alpha \odot a) \oplus (\alpha \odot b),$
5. $\forall \alpha, \beta \in T, \forall a \in V : (\alpha + \beta) \odot a = (\alpha \odot a) \oplus (\beta \odot a),$
6. $\forall a \in V : 1 \odot a = a,$
7. $\exists \theta \in V, \forall a \in V : 0 \odot a = \theta.$

*Prvky vektorového prostoru nazýváme **vektory**, prvky tělesa T nazýváme **skaláry**[12] a prvek θ z axiomu 7 nazýváme **nulový vektor**.*

Čtenář si jistě snadno sám zkontroluje, že pozorované vlastnosti šipek v $\mathbb{R}^2$ z pozorování 2.1 přesně odpovídají axiomům v definici 2.2.

Při definici vektorového prostoru musíme mít vždy ujasněn kontext, jak je zvolena množina V, těleso T, zobrazení $\oplus$ a $\odot$. Bude-li třeba, použijeme explicitně označení

$$(V, T, \oplus, \odot)\,.$$

[12] Ačkoli by se mohlo zdát divné, že obyčejnému „číslu“ říkáme skalár, má to svůj historický (geometrický důvod). Představme si pod pojmem vektor (v duchu dřívějších příkladů) orientovanou šipku v rovině či prostoru vedoucí z počátku soustavy souřadnic do nějakého bodu. Operace násobení číslem pak s takovou šipkou nedělá nic jiného, než že ji „prodlužuje či zkracuje“ (jinak také „škáluje“). Anglické *to scale* pak přirozeně vede k pojmu *scalar*, česky skalár.

Nesmíme se nechat vyvést z míry existencí dvou párů operací „plus“ a „krát“, pokud hrozí zmatení, je doporučeno je rozlišovat. Operace $+$ a $\cdot$ nám jsou „dodány“ spolu s tělesem, jsou součástí jeho definice. Vektorové operace $\oplus$ a $\odot$ pak přidáváme až jako součást definice vektorového prostoru a je dobré si uvědomit, že se od těch tělesových mohou více či méně lišit. Z důvodu úspornosti si však dovolíme značení zjednodušit – budeme-li mít jasno ve významech všech použitých symbolů, můžeme i vektorové operace značit klasickým[13] $+$ a $\cdot$.

Pouze pokud bude z kontextu naprosto jasné, kde se pohybujeme, lze vektorový prostor značit pouze V. Ve znění dokazovaných matematických vět pak často mluvíme pouze o *vektorovém prostoru V nad tělesem T* bez upřesnění operací. Obzvláště v delším textu pak budeme běžně zkracovat sousloví vektorový prostor jako **VP**.

Poznámka 2.3. *Je-li řeč o významu symbolů a rozlišování kontextu, musíme upozornit na jeden častý nešvar. Mezi oblíbené studentské hříchy totiž patří takové činy jako je „sčítání“ skaláru s vektorem, nebo „násobení“ vektoru vektorem – nic takového ale (zatím[14]) nemáme definováno, jde tedy o naprosté nesmysly. Podobně nemá smysl mluvit o součinu „vektor krát skalár“. Byť se to může zdá jako technická drobnost, při násobení vektoru skalárem nelze jen tak zaměňovat pořadí – toto půjde dobře vidět například u vektorového prostoru v příkladu 2.10.*

Poznámka 2.4. *Dalším oblíbeným kamenem úrazu je jistá vizuální „podobnost“ mezi axiomy tělesa a axiomy vektorového prostoru. Oboje musíme důsledně oddělovat. Vektorový prostor „budujeme“ vždy ve dvou krocích,*

1. *Nejprve zvolíme vhodné číselné těleso – jeho axiomy nám vlastně zaručují, že se skaláry „půjde rozumně pracovat“, viz definice 1.41.*

2. *Až poté zvolíme množinu vektorů a dvě vektorové operace, které z těch tělesových mohou vycházet, ale také nemusí. Až celá tato čtveřice dohromady (těleso se svými operacemi, množina vektorů, dvě vektorové operace) musí splňovat axiomy vektorového prostoru – tím máme zaručeno, že „půjde rozumně pracovat“ i s touto o stupeň složitější strukturou.*

Poznámka 2.5. *Abychom měli v používaných výrazech alespoň trochu pořádek a přehledno, pokusíme se o důsledné rozlišování skalárů a vektorů. Pro zápis vektorů (ať již konkrétních při výpočtech, nebo obecných ve zněních vět) budeme vždy používat malá písmena* ***latinské*** *abecedy, tedy*

$$a, b, c, \ldots, x, y, \ldots.$$

Oproti tomu skaláry – prvky číselných těles – budeme důsledně značit malými ***řeckými*** *písmeny,*

$$\alpha, \beta, \gamma, \delta, \ldots.$$

Tato konvence nás ale samozřejmě nijak neomezuje v používání indexů (α_1, x_n,...) jak u skalárů tak u vektorů!

[13] Mělo by nám být vždy jasné, jestli zrovna sčítáme dva skaláry nebo vektory, jestli násobíme dva skaláry nebo skalár s vektorem.

[14] Později si zavedeme různé součiny mezi vektory, tzv. skalární součin a vektorový součin. Prozatím ale žádný takový pojem k dispozici nemáme.

Jedinou výjimkou z tohoto pravidla bude občasné použití symbolů $x, y, z, t, \ldots$ jako neznámých v soustavě rovnic nebo jako složek vektorů z $\mathbb{R}^2$, $\mathbb{R}^3$ a tak dále (kde jsme z analytické geometrie zvyklí např. na značení $(x, y, z) \in \mathbb{R}^3$).

Ještě než přejdeme k základním příkladům vektorových prostorů, provedeme si jednoduché mentální cvičení – vyslovíme si naši první větu platnou pro libovolný vektorový prostor V nad obecným tělesem T, popisující několik důležitých vlastností nulového vektoru, a rovnou si ji i dokážeme. Přitom použijeme pouze axiomy vektorového prostoru, axiomy tělesa, případně již dříve dokázané body této věty[15].

Věta 2.6. *Buď V vektorový prostor nad tělesem T. Potom platí:*

(i) *Ve V existuje právě jeden nulový vektor.*

(ii) $\forall \alpha \in T : \alpha\theta = \theta$.

(iii) $\forall a \in V : a + \theta = a$.

(iv) *Ke každému vektoru z V existuje právě jeden* ***vektor opačný****. Tzn.,*

$$\forall a \in V, \exists_1 b \in V : a + b = \theta.$$

(v) $\forall \alpha \in T, \forall a \in V : (\alpha a = \theta \Rightarrow (\alpha = 0 \vee a = \theta))$.

Důkaz. Větu dokážeme přímo z axiomů vektorového prostoru, využití axiomu číslo n v rovnosti označíme $\overset{(An)}{=}$. Použití výsledku z předchozího bodu n této věty označíme $\overset{(n)}{=}$. V úpravách používáme také axiomy tělesa, ty explicitně nevyznačujeme.

(i) Nechť existují dva nulové vektory θ_1 a θ_2. Pak $\theta_1 \overset{(A7)}{=} 0 \cdot a \overset{(A7)}{=} \theta_2$, kde $a \in V$ je libovolné.

(ii) $\alpha \cdot \theta \overset{(A7)}{=} \alpha \cdot (0 \cdot a) \overset{(A3)}{=} (\alpha 0) \cdot a = 0 \cdot a \overset{(A7)}{=} \theta$, platí pro libovolné $\alpha \in T$ a $a \in V$.

(iii) $a + \theta \overset{(A6)}{=} 1 \cdot a + \theta \overset{(A7)}{=} 1 \cdot a + 0 \cdot a \overset{(A5)}{=} (1 + 0) \cdot a = 1 \cdot a \overset{(A6)}{=} a$, platí pro libovolné $a \in V$.

(iv) *Existence:* Buď $a \in V$. Položme $b := (-1) \cdot a$ (číslo opačné k 1 v tělese vždy existuje, označme jej -1). Potom

$$a + b = a + (-1) \cdot a \overset{(A6)}{=} 1 \cdot a + (-1) \cdot a \overset{(A5)}{=} (1 + (-1)) \cdot a = 0 \cdot a \overset{(A7)}{=} \theta.$$

Jednoznačnost: Nechť b_1 a b_2 jsou dva vektory opačné k $a \in V$, tedy $a + b_1 = a + b_2 = \theta$. Pak

$$\begin{aligned} b_1 &\overset{(3)}{=} b_1 + \theta = b_1 + (a + b_2) \overset{(A2)}{=} (b_1 + a) + b_2 \overset{(A1)}{=} (a + b_1) + b_2 = \theta + b_2 \\ &\overset{(A1)}{=} b_2 + \theta \overset{(3)}{=} b_2. \end{aligned}$$

(v) Nechť $\alpha a = \theta$, předpokládejme, že navíc platí $\alpha \neq 0$. Pak nutně dostáváme $a = \theta$, neboť

$$a \overset{(A6)}{=} 1 \cdot a = \left(\alpha^{-1}\alpha\right)a \overset{(A3)}{=} \alpha^{-1} \cdot (\alpha a) = \alpha^{-1} \cdot \theta \overset{(2)}{=} \theta.$$ □

[15] Bude nám tedy úplně jedno, jak dotyčný vektorový prostor vlastně vypadá. Slabší povahy nechť to považují za první demonstraci síly naší obecnosti.

Příklady vektorových prostorů

Jak jsme si už sáhodlouze ujasnili, naše definice vektorového prostoru je naprosto obecná a cokoli, co si v budoucnu dokážeme, bude platit pro všechny myslitelné vektorové prostory. Nicméně, protože máme v kurzu BI-LIN poněkud omezený prostor, při praktickém počítání se omezíme na několik základních typů vektorových prostorů, z nichž většinu už (neformálně) známe.

Fakt, že se jedná o vektorové prostory, ponecháváme bez důkazu. Věříme, že čtenář si snadno[16] ve všech případech splněnost axiomů VP dokáže. Dále zdůrazněme, že jakékoli sčítání či násobení, které je použito v definici vektorových operací (tj. „na pravé straně definujícího :=“) je mezi prvky tělesa – tedy závisí na volbě T a nemusí vůbec jít o „obyčejné“ sčítání a násobení.

Příklad 2.7. *Nechť T je libovolné těleso a $n \in \mathbb{N}$. Čtveřice*

$$(T^n, T, +, \cdot),$$

kde operace $+, \cdot$ definujeme po složkách, tedy pro každé $\alpha \in T$ a pro každé $x, y \in T^n$ platí

$$\begin{aligned} x + y = (x_1, \ldots, x_n) + (y_1, \ldots, y_n) &:= (x_1 + y_1, \ldots, x_n + y_n)\,, \\ \alpha x = \alpha(x_1, \ldots, x_n) &:= (\alpha x_1, \ldots, \alpha x_n)\,, \end{aligned}$$

je vektorový prostor.

Rozmyslete si, že triviální volba $n = 1$ v definici nijak nevadí, tedy i těleso samotné lze považovat (s danými operacemi) za vektorový prostor samo nad sebou! V prostorech typu $(T, T, +, \cdot)$ se nicméně pohybovat nebudeme, jednak nejsou příliš zajímavé a jednak při nich hrozí nejednoznačnosti v zápisech.

Přirozeným zobecněním a se znalostí maticových operací vyložených v části 1.5 snadno dojdeme k následujícímu příkladu.

Příklad 2.8. *Nechť T je libovolné těleso a $m, n \in \mathbb{N}$. Čtveřice*

$$(T^{m,n}, T, +, \cdot),$$

kde $T^{m,n}$ značí množinu všech obdélníkových matic o rozměru $m \times n$ s prvky z tělesa T a operace $+, \cdot$ definujeme po složkách, tedy pro každé $\alpha \in T$ a pro každé $x, y \in T^{m,n}$ platí

$$\begin{aligned} \forall i \in \hat{m}, \forall j \in \hat{n} : (x + y)_{ij} &:= x_{ij} + y_{ij}\,, \\ (\alpha x)_{ij} &:= \alpha x_{ij}\,, \end{aligned}$$

je vektorový prostor.

Příklad 2.9. *Nechť T je libovolné těleso, Symbolem T^∞ značíme množinu všech (nekonečných) posloupností prvků z tělesa T. Čtveřice*

$$(T^\infty, T, +, \cdot),$$

[16] A nadmíru ochotně.

kde operace $+, \cdot$ *definujeme po složkách, tedy pro každé* $\alpha \in T$ *a pro každé* $x, y \in T^\infty$ *platí*

$$x + y = (x_1, x_2, x_3, \dots) + (y_1, y_2, y_3, \dots) := (x_1 + y_1, x_2 + y_2, x_3 + y_3, \dots)\,,$$
$$\alpha x = \alpha(x_1, x_2, x_3, \dots) := (\alpha x_1, \alpha x_2, \alpha x_3, \dots)\,,$$

je vektorový prostor[17].

Závěrečný příklad této části není vyloženě „aplikovatelný“, ale zaslouží si zmínku. Jde totiž o velice jednoduchý příklad vektorového prostoru, ve kterém jsou vektorové operace $\oplus$ a $\odot$ voleny nestandardně.

Příklad 2.10. *Pro konstrukci vektorového prostoru volme následující „ingredience“:*

- $V = \mathbb{R}^+$, *vektory jsou kladná reálná čísla,*
- $T = \mathbb{R}$, *skaláry bereme z množiny všech reálných čísel,*
- *pro každé* $x, y \in \mathbb{R}^+$ *definujeme*

  $$x \oplus y := x \cdot y,$$

  kde $\cdot$ *značí klasické násobení reálných čísel,*
- *pro každé* $\alpha \in \mathbb{R}$ *a každé* $x \in \mathbb{R}^+$ *definujeme*

  $$\alpha \odot x := x^\alpha,$$

  kde v předpisu používáme standardní umocnění kladného reálného čísla na reálnou mocninu.

Čtveřice $(\mathbb{R}^+, \mathbb{R}, \oplus, \odot)$ *je vektorový prostor*[18].

Podprostor

Začněme jednoduchou naivní představou, která by nám měla posloužit jako motivace k zavedení nového pojmu *podprostor*[19]. Omezíme se přitom na těleso $\mathbb{R}$ reálných čísel. Jak jsme si už vysvětlili, $\mathbb{R}^n$ je pro každé $n \in \mathbb{N}$ vektorovým prostorem. Ten „nejmenší“ z nich, $\mathbb{R}^1$ si můžeme jednoduše představit jako přímku s označeným počátkem $\theta = 0$, jednotlivé vektory pak odpovídají buďto bodům na přímce, nebo orientovaným úsečkám vedoucím z θ do nějakého bodu na přímce.

Podíváme-li se stejným způsobem na $\mathbb{R}^2$, dostaneme rovinu s počátkem $\theta = (0, 0)$[20]. V této rovině je přitom „obsažen“ celý předchozí prostor $\mathbb{R}^1$ – například jako osa x (v řeči pravoúhlého systému souřadnic (x, y)). Jinými slovy, každý vektor

[17] Fakt, že množina nekonečných posloupností vybavena sčítáním a násobením číslem po složkách je vektorový prostor, jistě oceníme v kurzu BI-ZDM – umožní nám totiž vyslovit některá zásadní tvrzení pro řešení tzv. lineárních rekurentních rovnic.

[18] Čtenáři důrazně doporučujeme, aby se vnitřně obohatil vlastním pokusem o důkaz toho, že se skutečně o vektorový prostor jedná.

[19] Pro jistotu opět zopakujme: motivační naivní představa nerovná se přesná definice!

[20] De facto zde opakujeme část 2.2, opakování je ale matka moudrosti.

$a \in \mathbb{R}^1$ lze v jistém smyslu považovat i za vektor v $\mathbb{R}^2$, konkrétně jako $(a, 0) \in \mathbb{R}^2$. Podobně bychom mohli postupovat dále a konstatovat, že v $\mathbb{R}^3$ je v jistém smyslu obsažen jak celý prostor $\mathbb{R}^1$, tak i celý $\mathbb{R}^2$ (například jako rovina určená osami x a y s korespondencí $(a, b) \in \mathbb{R}^2 \leftrightarrow (a, b, 0) \in \mathbb{R}^3$)[21].

Ideálně jsme teď tedy mohli nabýt správného dojmu, že různé vektorové prostory nemusí nutně být „každý z jiného světa“, ale že spolu mohou nějak souviset. Konkrétně, mohou být celé obsaženy v jiných, „větších“, vektorových prostorech a samy mohou i jiné vektorové prostory obsahovat jako své podmnožiny. Toť naší motivací pro pojem *podprostor*.

Definice 2.11. *Nechť V je vektorový prostor nad tělesem T a nechť $\emptyset \neq P \subset V$ (P je neprázdná podmnožina V). Říkáme, že P je **podprostor** prostoru V, právě když platí:*

1. $\forall x, y \in P\colon x + y \in P$,

2. $\forall \alpha \in T, \forall x \in P\colon \alpha x \in P$

*(tedy P je množina **uzavřená** na obě vektorové operace $+, \cdot$). Vztah „být podprostorem“ pak značíme*

$$P \subset\subset V.$$

Poznamenejme, že tato definice lze zapsat mnohem elegantněji s využitím množinových operací z definice 1.20: *Nechť V je VP nad T a P je jeho neprázdná podmnožina. Pak řekneme, že P je podprostorem V pokud současně platí*

$$P + P \subseteq P \quad \text{a} \quad T \cdot P \subseteq P.$$

Jak si mohl pozorný čtenář všimnout, v celé definici podprostoru nepadlo ani slovo o vlastnosti „být také vektorovým prostorem“. To není žádný omyl, definice pomocí uzavřenosti na vektorové operace je prostě jednodušší a snadno ověřitelná. Souvislost s úvodní motivací nám poskytne následující věta.

Věta 2.12. *Nechť V je vektorový prostor nad tělesem T, nechť $P \subset\subset V$. Potom P se zúžením[22] operace sčítání vektorů $+$ na $P \times P$ a operace násobení vektorů skalárem $\cdot$ na $T \times P$ je také vektorový prostor nad T.*

Důkaz. Označme zúžení operací $+, \cdot$ na $P \subset\subset V$ jako $+|_P, \cdot|_P$. Ověříme podmínky pro to, aby $(P, T, +|_P, \cdot|_P)$ byl vektorovým prostorem, dle definice 2.2:

- Uzavřenost operací $+|_P : P \times P \to P$ a $\cdot|_P : T \times P \to P$ plyne rovnou z definice podprostoru.

- Jelikož axiomy vektorového prostoru platí pro každé $\alpha, \beta \in T$ a $a, b, c \in V$, platí nutně i pro každé $a, b, c \in P \subseteq V$. Tím máme pro P dokázáno splnění axiomů 1 až 6.

[21] S touto představou samozřejmě můžeme pokračovat v libovolném $\mathbb{R}^n$, ale není třeba to s motivací přehánět...

[22] Netřeba se cítit zaskočen pojmem *zúžené* zobrazení, ten znáte dobře například z BI-ZMA! Jde jednoduše o zobrazení, kterému je uměle nahrazen definiční obor nějakou jeho podmnožinou. Tedy v případě sčítání $+$ zužujeme z $V \times V$ na $P \times P \subset V \times V$.

- Z axiomu 7 pro V a z předchozího bodu plyne, že bude-li nulový vektor $\theta \in V$ současně ležet v podprostoru P, bude i v něm hrát roli nulového vektoru a i poslední axiom bude pro P splněn. Pro každé $a \in P \subseteq V$ ovšem platí $0 \cdot a = \theta$ a jelikož P je uzavřený na násobení skalárem, skutečně platí $\theta \in P$[23]. $\square$

S uvedením konkrétních příkladů ještě chvíli počkáme, řekneme si nejprve pár základních vlastností podprostorů.

Pozorování 2.13. *Buď V vektorový prostor nad T a nechť $P \subset\subset V$. Pak platí:*

1. *$\theta \in P$.*
2. *$\{\theta\} \subset\subset V$ a $V \subset\subset V$.*
3. *Pro každou podmnožinu $P_1 \subseteq P$ platí implikace: $P_1 \subset\subset P \Rightarrow P_1 \subset\subset V$.*

Ponecháme na čtenáři, aby si tyto jednoduché vlastnosti odůvodnil[24]. Pouze poznamenáme, že např. bod 3 už byl vlastně dokázán – během důkazu věty 2.12.

Definice 2.14. *Podprostory $\{\theta\}$ a V vektorového prostoru V nazýváme* ***triviálními podprostory****. Každý podprostor $P \subset\subset V$ pro který současně platí $P \neq V$ nazýváme* ***vlastním podprostorem***[25].

Poznámka 2.15. *Ačkoli první bod v pozorování 2.13 vypadá nevinně, je velmi praktický, chceme-li dokázat, že nějaká množina podprostorem* ***není****. Víme, že implikaci obecně nelze obrátit, ale lze ji tzv. obměnit, $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$. Tedy zatímco fakt $\theta \in P$ pro nějakou podmnožinu $P \subseteq V$ rozhodně* ***nestačí*** *na to, aby P byla podprostorem, můžeme s klidným srdcem říci, že*

$$\theta \notin P \Rightarrow P \text{ není podprostorem } V\,.$$

Příklad 2.16. *V $\mathbb{R}^2$ jsou jedinými netriviálními podprostory přímky procházející počátkem $\theta = (0, 0)$, například*

$$P = \{(x, y) \in \mathbb{R}^2 \mid x + 2y = 0\} \subset\subset \mathbb{R}^2\,.$$

Přímky, které neprocházejí počátkem, nemohou být podprostory.

Příklad 2.17. *V $\mathbb{R}^3$ jsou jedinými netriviálními podprostory přímky a roviny procházející počátkem $\theta = (0, 0, 0)$, například*

$$\begin{aligned} P_1 =& \{(x, y, z) \in \mathbb{R}^3 \mid x + 2y = 0 \wedge z = 0\} \subset\subset \mathbb{R}^3\,,\\ P_2 =& \{(x, y, z) \in \mathbb{R}^3 \mid x + 2y = 0\} \subset\subset \mathbb{R}^3\,,\\ P_3 =& \{(x, y, z) \in \mathbb{R}^3 \mid 2x + y - z = 0\} \subset\subset \mathbb{R}^3\,. \end{aligned}$$

Rovina či přímka, která neprochází počátkem, nemůže být podprostor. Např. množina

$$\{(x, y, z) \in \mathbb{R}^3 \mid 2x + y - z = 3\} \quad \text{není podprostor } \mathbb{R}^3\,.$$

[23] Perfekcionista na tomto místě správně doplní, že takové $a \in P$ vůbec existuje – neboť P je z definice neprázdná množina.

[24] Tak, aby je byl schopen odůvodnit i případnému zkoušejícímu.

[25] Jen aby bylo jasno: netriviální podprostor není totéž, co vlastní podprostor. Platí, že každý vlastní podprostor je buďto netriviální, nebo obsahuje jen nulový vektor.

Ke klasifikaci podprostorů v $\mathbb{R}^3$ lze dojít i následující naivní úvahou. Dejme tomu, že chceme zkonstruovat všechny možné podprostory v $\mathbb{R}^3$, rozeberme si, jaké máme možnosti:

(i) Každý podprostor musí obsahovat nulový vektor θ – nejmenším podprostorem je zřejmě ten triviální, $\{\theta\}$.

(ii) Každý netriviální podprostor musí kromě θ obsahovat ještě nějaký další bod, přidejme tedy nějaké $a \in \mathbb{R}^3$. Jenže podprostor musí být uzavřený na vektorové $+, \cdot$, to zřejmě zajistíme přidáním všech násobků $\alpha a, \alpha \in \mathbb{R}$. V závislosti na volbě $a \in \mathbb{R}$ tak dostaneme libovolnou přímku procházející počátkem.

(iii) Abychom dostali ještě větší podprostor, vezmeme libovolnou přímku procházející počátkem a přidáme k ní bod, který v ní neleží. Chceme-li pak zařídit uzavřenost výsledné množiny na vektorové operace, musíme do ní přidat všechny reálné násobky přidaného bodu a ještě k tomu všechny součty bodů na původní přímce a nově přidaných. Rozmyslete si, že tím vždy získáme nějakou rovinu, která prochází počátkem.

(iv) Poslední možností je vzít nějakou rovinu z bodu (iii) a přidat k ní nějaký bod, který v ní neleží, a opět zajistit uzavřenost na operace. Tím ovšem získáme triviální podprostor – celé $\mathbb{R}^3$.

Poznámka 2.18. *Celá předchozí úvaha stála na jednoduché geometrické představě „třírozměrného prostoru“ – ta je na obecný vektorový prostor krátká. Podotkněme, že jsme přitom už vlastně některé pojmy z lineární algebry použili (aniž bychom o nich věděli), oba si pořádně zadefinujeme v částech 2.4 a 2.5:*

- *Při přidávání nových bodů k podprostorům jsme využívali formulace „neleží na stejné přímce nebo ve stejné rovině“, toto souvisí s obecnějším pojem* lineární nezávislost*.*
- *Při zajišťování uzavřenosti na vektorové operace jsme přidávali všechny možné součty a násobky už obsažených vektorů. Tuto humpoláckou formulaci v budoucnu nahradíme sofistikovanějším pojmem – konstrukce* lineárního obalu *množiny.*

Podprostory jsou mimo jiné obyčejné podmnožiny nějakého V. Můžeme na ně tedy aplikovat různé množinové operace, jmenovitě například průnik, sjednocení a součet (viz definice 1.20) a zkoumat, zda je výsledek také podprostorem[26]. Než vyslovíme obecnou větu, uveďme jednoduchý příklad.

Příklad 2.19. *Uvažujme následující podprostory v $\mathbb{R}^2$:*

$$E_1 := \mathbb{R} \times \{0\} = \{(x,0) \mid x \in \mathbb{R}\},$$
$$E_2 := \{0\} \times \mathbb{R} = \{(0,y) \mid y \in \mathbb{R}\}.$$

Dle definic snadno odvodíme, že

[26] Operace vynásobení podprostoru číslem z tělesa nás nebude nijak zajímat. Zamyslete se sami, co triviálně platí pro libovolný podprostor (nejen $\mathbb{R}^3$ nad $\mathbb{R}$, ale obecně), když ho vynásobíme dle definice libovolným $\alpha \in T$!

(i) $E_1 \cap E_2 = \{(0,0)\}$ *je podprostor.*

(ii) $E_1 \cup E_2 = \{(x,y) \in \mathbb{R}^2 \mid x = 0 \vee y = 0\}$ *není podprostor. Skutečně, obsahuje například vektory* $(1,0)$ *a* $(0,1)$*, ale už ne jejich součet* $(1,1)$*.*

(iii) $E_1 + E_2 = \{(x,0) + (0,y) \mid x, y \in \mathbb{R}\} = \mathbb{R}^2$ *je podprostor.*

Bod (ii) v předchozím příkladu nám poslouží jako protipříklad. Našli jsme dvojici podprostorů v nějakém VP, jejichž sjednocení není podprostor – tedy tvrzení „Sjednocení libovolných dvou podprostorů v libovolném VP je také podprostor“ **není pravdivé**. Naopak body (i) a (iii) nám mohou naznačit, že v případě průniku a součtu podprostorů bude situace příznivější – ale vzhledem k tomu, že máme k dispozici jen konkrétní příklad, příslušná tvrzení budeme muset dokázat obecně.

Poznamenejme ještě, že tvrzení věty níže lze rozšířit i na operace s více podprostory, než jen se dvěma – pro pochopení nám ale postačí tato jednodušší varianta.

Věta 2.20. *Buď* V *vektorový prostor nad tělesem* T*, nechť* P *a* Q *jsou libovolné podprostory* V*. Pak platí následující:*

(i) $P \cap Q \subset\subset V$.

(ii) $P \cup Q$ *nemusí být podprostorem.*

(iii) $P + Q \subset\subset V$.

Důkaz. (i) Jelikož $P, Q \subseteq V$ a oba obsahují alespoň nulový vektor θ, zřejmě platí $P \cap Q \subseteq V$ i $P \cap Q \neq \emptyset$. Ověříme, že pro každé $\alpha \in T$ a $x, y \in P \cap Q$ platí $x + y \in P \cap Q$ a současně $\alpha x \in P \cap Q$:

Nechť $\alpha \in T$ a $x, y \in P \cap Q$ jsou libovolné. Pak snadno odvodíme, že

$$\begin{aligned} (x, y \in P \wedge x, y \in Q) &\overset{P,Q \subset\subset V}{\Rightarrow} (x + y \in P \wedge x + y \in Q) \Rightarrow (x + y \in P \cap Q), \\ &\overset{P,Q \subset\subset V}{\Rightarrow} (\alpha x \in P \wedge \alpha x \in Q) \Rightarrow (\alpha x \in P \cap Q), \end{aligned}$$

což znamená, že $P \cap Q$ je podprostor.

(ii) Plyne z existence protipříkladu, viz příklad 2.19.

(iii) Součet $P+Q$ je zřejmě neprázdný neboť $\theta \in P$ a $\theta \in Q$, tedy $\theta = \theta + \theta \in P + Q$. Nechť $\alpha \in T$ a $x, y \in P + Q$, přičemž

$$x = a_1 + b_1\,,\ \ y = a_2 + b_2\,,$$

kde $a_i \in P, b_i \in Q$ pro $i \in \{1, 2\}$. Protože

$$\begin{aligned} x + y &= (a_1 + b_1) + (a_2 + b_2) = \underbrace{(a_1 + a_2)}_{\in P} + \underbrace{(b_1 + b_2)}_{\in Q}\,, \\ \alpha x &= \alpha(a_1 + b_1) = \underbrace{\alpha a_1}_{\in P} + \underbrace{\alpha b_1}_{\in Q}\,, \end{aligned}$$

kde jsme využili faktu, že P i Q jsou podprostory, platí $x + y \in P + Q$ i $\alpha x \in P + Q$, tedy $P + Q \subset\subset V$. □

Poznámka 2.21. *Zvídavý čtenář by si mohl položit otázku, jestli existuje nějaká další podmínka, která zaručí, že sjednocení nějakých dvou podprostor už nutně podprostor je. Uvádíme ji jen pro úplnost a i její důkaz ponecháváme pouze na iniciativě čtenářů. Jsou-li $P, Q \subset\subset V$, pak platí*

$$P \cup Q \subset\subset V \Leftrightarrow (P \subseteq Q) \vee (Q \subseteq P).$$

2.4 Lineární (ne)závislost

V této části se poprvé objeví slovní spojení **soubor vektorů (délky n)**, s typickým značením

$$(x_1, x_2, \dots, x_n), \text{ kde } x_i \in V \text{ pro každé } i \in \hat{n}\,.$$

Je to něco jiného než množina vektorů – na rozdíl od ní se na soubor vektorů díváme jako na uspořádanou $n$tici[27]. Navíc množina nemusí být nutně **konečná**!

Poznámka 2.22. *Důrazně upozorněme na jeden oblíbený problém se značením. Napíšeme-li bez kontextu pouze $(x_1, x_2, \dots, x_n)$, může to znamenat minimálně tyto dvě různé věci! A to:*

1. *Soubor vektorů, pokud $x_1, x_2, \dots, x_n$ jsou postupně očíslované vektory v nějakém VP V. Toto je třeba správně zapsat jako $(x_1, x_2, \dots, x_n) \subseteq V$, případně slovně: „Nechť $(x_1, x_2, \dots, x_n)$ je soubor vektorů z V.“*

2. *Jeden jediný vektor z nějakého vektorového prostoru typu T^n, tedy vektor, jehož složkami jsou popořadě $x_1, x_2, \dots, x_n \in T$. V tom případě musíme použít správný zápis $(x_1, x_2, \dots, x_n) \in V$, $\subseteq$ vs. $\in$. pro $V = T^n$.*[28]

Definice 2.23. *Nechť V je vektorový prostor nad T, $x \in V$ a $(x_1, \dots, x_n)$ je soubor vektorů z V. Říkáme, že vektor x je **lineární kombinací** souboru $(x_1, \dots, x_n)$, právě když existují čísla $\alpha_1, \dots, \alpha_n \in T$ taková, že*[29]

$$x = \sum_{i=1}^{n} \alpha_i x_i.$$

*Čísla α_i, $i \in \hat{n}$, nazýváme **koeficienty lineární kombinace**. Jestliže $\forall i \in \hat{n} : \alpha_i = 0$, nazýváme takovou lineární kombinaci **triviální**. V opačném případě jde o lineární kombinaci **netriviální**.*

O triviálních lineárních kombinacích lze rovnou odvodit, že se vždy rovnají nulovému vektoru θ. Pokuste se to sami dokázat, nebudete přitom potřebovat nic jiného, než základní vlastnosti nulových vektorů.

[27] Zatím na tom pořadí moc nesejde, ale až se dostaneme k pojmu *báze*, bude se nám uspořádání vektorů v souboru náramně hodit.

[28] V podstatě se jedná o oblíbený konflikt „náležítko vs. podmnožinítko“

[29] V této sumě se vektory x_i násobí skaláry a tyto výsledky se pak sčítají – nikoho by nemělo překvapit, že se zde sčítá a násobí podle obecných operací z definice vektorového prostoru!

Definice 2.24. *Nechť* $(x_1, \dots, x_n)$ *je soubor vektorů z* V. *Řekneme, že* $(x_1, \dots, x_n)$ *je* ***lineárně nezávislý (LN)*** *soubor, právě když pouze triviální lineární kombinace tohoto souboru je rovna nulovému vektoru* θ. *V opačném případě nazýváme soubor* ***lineárně závislý (LZ)****.*

Jinými slovy[30]*:*

- $(x_1, \dots, x_n)$ *je LN* $\Leftrightarrow$

$$\forall \alpha_1, \dots, \alpha_n \in T : \left(\sum_{i=1}^{n} \alpha_i x_i = \theta \Rightarrow (\forall i \in \hat{n})(\alpha_i = 0) \right)$$

- $(x_1, \dots, x_n)$ *je LZ* $\Leftrightarrow$

$$\exists \alpha_1, \dots, \alpha_n \in T, \exists i \in \hat{n}, \alpha_i \neq 0 : \left(\sum_{i=1}^{n} \alpha_i x_i = \theta \right)$$

Tedy lineárně nezávislé soubory jsou soubory takových vektorů, ze kterých není možné (pomocí násobení skaláry a sčítání vektorů mezi sebou) vyrobit nulový vektor – tedy jiným než triviálním způsobem (jako triviální lineární kombinaci). V jiných kurzech lineární algebry můžete narazit na definici jinou, se zněním: *Soubor vektorů je LZ právě tehdy, pokud je jeden z vektorů souboru lineární kombinací ostatních.* My se ale v našem kurzu budeme držet definice 2.24, protože se (jak si brzy ukážeme) mnohem snadněji ověřuje! Později, ve větě 2.36 si navíc dokážeme, že jsou obě charakterizace lineární (ne)závislosti ekvivalentní.

Pozorování 2.25. *Následující jednoduché vlastnosti (především „malých“) souborů vektorů, lze odvodit přímo z definice 2.24:*

(i) Lineární (ne)závislost nezávisí na pořadí vektorů v souboru.

(ii) Obsahuje-li soubor dva stejné vektory, potom je LZ.

(iii) Obsahuje-li soubor nulový vektor, potom je LZ.

(iv) Soubor délky 1 je LZ, právě když je tvořen nulovým vektorem.

(v) Soubor délky 2 je LZ, právě když jeden vektor je násobkem druhého.

(vi) Přidáním vektoru do LZ souboru vznikne LZ soubor.

(vii) Odebráním vektoru z LN souboru vznikne LN soubor.

Můžeme si společně okomentovat[31] například body (ii) a (vi), zbytek si laskavý čtenář ověří doma sám.

[30] Jazykem predikátové logiky.
[31] Tedy dokázat…

(ii): Předpokládejme, že soubor $(x_1, \dots, x_n)$ splňuje $x_k = x_\ell$ pro nějaké dva indexy $k, \ell \in \hat{n}, k \neq \ell$. Zvolíme-li koeficienty lineární kombinace tak, aby platilo

$$\alpha_k = 1, \alpha_\ell = -1, \text{ a } \alpha_i = 0 \text{ pro každé } i \in \hat{n} \setminus \{k, \ell\}^{32},$$

bude se jednat o netriviální lineární kombinaci, která současně splňuje

$$\sum_{i=1}^{n} \alpha_i x_i = 1x_k + (-1)x_\ell = \theta\,.$$

(vi): Je-li soubor $(x_1, \dots, x_n)$ LZ, existují koeficienty $\alpha_1, \dots, \alpha_n \in T$, z nichž aspoň jeden je nenulový, takové, že

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = \theta\,.$$

Přidáme-li do souboru libovolný vektor, označme jej x_{n+1}, dostaneme volbou $\alpha_{n+1} = 0$ netriviální[33] lineární kombinaci, splňující

$$\alpha_1 x_1 + \cdots + \alpha_n x_n + \underbrace{\alpha_{n+1} x_{n+1}}_{=\theta} = \alpha_1 x_1 + \cdots + \alpha_n x_n = \theta\,,$$

tedy soubor zůstává i po přidání x_{n+1} stále LZ.

Příklad 2.26. *Na pojem lineární nezávislosti můžeme přirozeně nahlížet, jako na jisté zobecnění známých geometrických vlastnost bodů „neležet v jedné přímce / v jedné rovině“, jak už jsme lehce prozradili v poznámce 2.18. Konkrétně platí následující:*

- *Dvě orientované úsečky v $\mathbb{R}^2$ (nebo $\mathbb{R}^3$) leží v jedné přímce, právě když jsou odpovídající vektory LZ.*
- *Tři orientované úsečky v $\mathbb{R}^3$ leží v jedné rovině, právě když jsou odpovídající vektory LZ.*
- *Soubor vektorů z $\mathbb{R}^2$ délky 3 je vždy LZ.*
- *Soubor vektorů z $\mathbb{R}^3$ délky 4 je vždy LZ.*

Velice častou úlohou v lineární algebře je ověření, zda je zadaný soubor vektorů lineárně závislý nebo nezávislý. Vždy můžeme postupovat přesně podle definice 2.24:

Algoritmus 2.27 (Ověření LN/LZ souboru vektorů). *Pro zadaný soubor vektorů $(x_1, \dots, x_n)$ ve VP V ověřte, zda je LN nebo LZ.*

1. *Hledáme, jestli existuje i jiná ntice koeficientů $\alpha_1, \dots, \alpha_n \in T$ než $(0, \dots, 0)$ taková, že příslušná lineární kombinace je rovna nulovému vektoru.*

[32] Takto lze vždy koeficienty zvolit! Jednotkový prvek, značený 1, je obsažen v jakémkoli tělese T, prvek k němu opačný, -1, také.

[33] Protože alespoň jeden z původních koeficientů $\alpha_1, \dots, \alpha_n$ je nenulový.

2. *Koeficienty $\alpha_1, \dots, \alpha_n \in T$ považujme za neznámé v rovnici*

$$\alpha_1 x_1 + \dots + \alpha_n x_n = \theta.$$

3. *Z definice vektorových operací rovnici výše převeďme na soustavu lineárních rovnic (přesný postup závisí na konkrétní volbě prostoru $(V, T, +, \cdot)$), tato soustava nám vyjde vždy homogenní.*[34]

4. *Soustavu převeďme pomocí GEM do horního stupňovitého tvaru. Dle věty 1.28 určeme, kolik existuje řešení.*

5. *Existuje-li jediné řešení $(\alpha_1, \dots, \alpha_n) = (0, \dots, 0)$, je zadaný soubor LN, v opačném případě je LZ.*

Výše popsaný univerzální postup předvedeme na příkladech:

Příklad 2.28. *Vyšetříme lineární nezávislost souboru $((1,2,3),(4,7,8),(3,4,2))$ v $\mathbb{R}^3$.*

Hledáme koeficienty $\alpha, \beta, \gamma \in \mathbb{R}$ takové, že platí

$$\alpha(1,2,3) + \beta(4,7,8) + \gamma(3,4,2) = \theta = (0,0,0)\,.$$

Z definice vektorových operací pak dostáváme rovnost dvou vektorů z $\mathbb{R}^3$,

$$(\alpha + 4\beta + 3\gamma, 2\alpha + 7\beta + 4\gamma, 3\alpha + 8\beta + 2\gamma) = (0,0,0)\,,$$

která vede na soustavu lineárních rovnic v proměnných $\alpha, \beta, \gamma \in \mathbb{R}$.

Úpravou pomocí GEM pak dostáváme

$$\left(\begin{array}{ccc|c} 1 & 4 & 3 & 0 \\ 2 & 7 & 4 & 0 \\ 3 & 8 & 2 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 4 & 3 & 0 \\ 0 & -1 & -2 & 0 \\ 0 & -4 & -7 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 4 & 3 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right).$$

Jelikož se jedná o soustavu, jejíž rozšířená matice má jediný vedlejší sloupec (ten pravých stran), existuje právě jedno řešení $(\alpha, \beta, \gamma) = (0,0,0)$ a zadaný soubor je LN.

Příklad 2.29. *Vyšetříme lineární nezávislost souboru*

$$\left(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right) \quad v\ \mathbb{Z}_3^{2,2}.$$

Hledáme koeficienty $\alpha, \beta, \gamma, \delta \in \mathbb{Z}_3 = \{0,1,2\}$ takové, že platí

$$\alpha \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} + \beta \begin{pmatrix} 0 & 2 \\ 0 & 1 \end{pmatrix} + \gamma \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} + \delta \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \theta = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

[34] Zatím nemáme přesně zdůvodněno proč, ale souvisí to s faktem, že triviální lineární kombinace je vždy rovna nulovému vektoru, tedy že $(\alpha_1, \dots, \alpha_n) = (0, \dots, 0)$ je vždy jedno z řešení...

Z definice vektorových operací pak dostáváme rovnost dvou vektorů z $\mathbb{Z}_3^{2,2}$,

$$\begin{pmatrix} \alpha+\gamma & 2\beta+\delta \\ \alpha+\gamma & \alpha+\beta+2\gamma \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

která vede na soustavu lineárních rovnic v proměnných $\alpha, \beta, \gamma, \delta \in \mathbb{Z}_3$.

Úpravou pomocí GEM[35] *pak dostáváme*

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

Jelikož se jedná o soustavu, jejíž rozšířená matice má kromě posledního ještě jeden vedlejší sloupec, existuje více než jedno řešení, konkrétně platí, že $(\alpha, \beta, \gamma, \delta) \in \{(0,0,0,0), (1,1,2,1), (2,2,1,2)\}$. *Zadaný soubor je tedy LZ.*

Na závěr této části si dovolíme přidat ještě jednu definici lineární (ne)závislosti. Pozor ale, nepůjde o žádnou další alternativní definici či ekvivalentní tvrzení, nýbrž o zobecnění! Doposud máme LN/LZ definovánu pro konečné soubory vektorů, což nám většinou stačí. Nicméně, v části 2.6 budeme potřebovat pojem lineární nezávislosti rozšířit obecně na množiny, které mohou být i nekonečné.

Definice 2.30. *Buď* V *vektorový prostor nad* T, $\emptyset \neq M \subset V$. *Řekneme, že* M *je* ***lineárně závislá (LZ) množina****, právě když existují vektory* $x_1, \ldots, x_n \in M$ *takové, že* $x_i \neq x_j$ *pro* $i \neq j$, *kde* $i, j \in \hat{n}$, *a soubor* $(x_1, \ldots, x_n)$ *je LZ. V opačném případě je množina* M ***lineárně nezávislá (LN)****.*

Tato definice se dá ekvivalentně přeformulovat i takto: *Množina je lineárně nezávislá právě tehdy, když každý konečný soubor různých vektorů z ní je lineárně nezávislý.* Věříme, že si pozorný čtenář tuto reformulaci důkladně rozmyslí – jde jen o negaci výroku s kvantifikátory.

Současně pak vyzýváme ke krátkému rozjímání nad tím, jak spolu definice 2.24 a 2.30 souvisí. Měli bychom dojít k závěru, že poslední definice tu původní skutečně rozšiřuje – v tom smyslu, že pokud se v souboru $(x_1, \ldots, x_n)$ neopakují vektory a za M zvolíme množinu $\{x_1, \ldots, x_n\}$, obě definice budou ekvivalentní[36].

2.5 Lineární obal

Definice 2.31. *Buď* $(x_1, \ldots, x_n)$ *soubor vektorů z* V. *Množinu všech lineárních kombinací tohoto souboru nazveme* ***lineárním obalem souboru*** $(x_1, \ldots, x_n)$ *a značíme ji*

$$\langle x_1, \ldots, x_n \rangle.$$

[35] Pozor, pracujeme v $\mathbb{Z}_3$!

[36] Jen pro jistotu, ekvivalence dvou definic znamená, že jedna označí za LN právě tytéž konečné množiny (soubory), jako druhá.

Buď $\emptyset \neq M \subset V$. Množinu všech lineárních kombinací všech souborů vektorů z množiny M[37] *nazveme* ***lineárním obalem množiny*** *M a značíme ji $\langle M \rangle$.*

Pozorný čtenář si nyní jistě vzpomene na poznámku 2.18 a uvědomí si, že když jsme konstruovali jednoduché podprostory obohacováním množin o všechny myslitelné (konečné) lineární kombinace jejich vektorů, vyráběli jsme vlastně jejich lineární obaly.

Před uvedením ilustračních příkladů si jen vyslovme jednoduché pozorování, jehož důkaz můžeme opět nechat z velké části na čtenáři.

Pozorování 2.32. *Nechť M je libovolná podmnožina vektorového prostoru V. Pak platí:*

(i) $\theta \in \langle M \rangle$,

(ii) $M \subseteq \langle M \rangle$,

(iii) $x \in \langle M \rangle \Rightarrow \langle M \rangle = \langle M \cup \{x\} \rangle$,

(iv) $M \subseteq N \Rightarrow \langle M \rangle \subseteq \langle N \rangle$,

(v) $x, y \in \langle M \rangle \ \wedge\ \alpha \in T \Rightarrow x + y \in \langle M \rangle \ \wedge\ \alpha x \in \langle M \rangle$.

Dokážeme si společně jen část bodu (v): Předpokládejme, že $x, y \in \langle M \rangle$, tedy x je lineární kombinací nějakého souboru z V a stejně tak i y (i když může jít o jiný soubor vektorů). Z těchto dvou souborů udělejme sjednocení a výsledný soubor (vektory přitom libovolně seřaďme) označme $(z_1, z_2, \ldots, z_m)$. Potom ovšem existují koeficienty $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m \in T$ (některé z nich mohou být nulové, to nám nijak nevadí) takové, že platí,

$$\left(x = \sum_{i=1}^{m} \alpha_i z_i\right) \wedge \left(y = \sum_{i=1}^{m} \beta_i z_i\right) \Rightarrow (x + y) = \sum_{i=1}^{m} \underbrace{(\alpha_i + \beta_i)}_{\in T} z_i \,.$$

Tedy $x + y \in \langle M \rangle$ a uzavřenost na násobení skalárem lze dokázat analogicky.

Příklad 2.33. *Lineární obaly souborů vektorů v prostorech $\mathbb{R}^2$ a $\mathbb{R}^3$ vypadají následovně:*

- *Lineární obal nulového vektoru (počátku) je množina pouze s počátkem.*
- *Lineární obal nenulového vektoru z $\mathbb{R}^2$ (nebo z $\mathbb{R}^3$) je množina všech vektorů ležících ve společné přímce.*
- *Lineární obal LN souboru dvou vektorů z $\mathbb{R}^2$ je celé $\mathbb{R}^2$.*
- *Lineární obal LN souboru dvou vektorů z $\mathbb{R}^3$ je množina všech vektorů ležících ve společné rovině.*

[37] Důrazně připomeňme, že soubor vektorů je automaticky konečný. V lineární algebře se nesetkáme s ničím, jako nekonečný součet, tedy nikde neuvidíte symbol $\sum_{i=1}^{\infty}$. Abychom se mohli takovými součty zabývat, museli bychom ještě náš vektorový prostor vybavit strukturou podpírající konvergenci (tj. topologií). Tak daleko se ale nedostaneme.

- *Lineární obal LN souboru tří vektorů z $\mathbb{R}^3$ je celé $\mathbb{R}^3$.*

Příklad 2.34. *Na jednoduchém příkladu můžeme ilustrovat, jak moc i při konstrukci lineárního obalu záleží na konkrétním tělese. Nechť*

$$x_1 = (1,0,1,0), \quad x_2 = (0,1,1,0) \in T^4,$$

označme jejich lineární obal $L = \langle x_1, x_2 \rangle$. Vyjádříme, jak vypadá libovolný prvek $w \in L$, v závislosti na tělese T:

Vždy platí, že

$$\begin{aligned} w \in L &\Leftrightarrow \exists \alpha, \beta \in T : w = \alpha(1,0,1,0) + \beta(0,1,1,0), \\ &\Leftrightarrow w \in \{(\alpha, \beta, \alpha+\beta, 0) \mid \alpha, \beta \in T\}. \end{aligned}$$

- *Pro nekonečné těleso T ($\mathbb{C}, \mathbb{R}, \mathbb{Q}$) nic moc dalšího dělat nelze. Máme prvky L parametrizované pomocí $\alpha, \beta \in T$ libovolných.*
- *V případě konečných těles je pouze konečně možností pro volby $\alpha, \beta \in T$, můžeme tedy dosazováním získat všechny prvky L:*

  Je-li $T = \mathbb{Z}_2$:

$$\begin{aligned} L &= \{(\alpha, \beta, \alpha+\beta, 0) \mid \alpha, \beta \in \{0,1\}\} \\ &= \{(0,0,0,0), (0,1,1,0), (1,0,1,0), (1,1,0,0)\} \end{aligned}$$

  Je-li $T = \mathbb{Z}_3$:

$$\begin{aligned} L &= \{(\alpha, \beta, \alpha+\beta, 0) \mid \alpha, \beta \in \{0,1,2\}\} \\ &= \{(0,0,0,0), (0,1,1,0), (0,2,2,0), (1,0,1,0), (1,1,2,0), \\ &\qquad (1,2,0,0), (2,0,2,0), (2,1,0,0), (2,2,1,0)\} \end{aligned}$$

Leckoho mohla trknout jistá podobnost mezi příklady různých lineárních obalů a mezi popisem možných podprostorů v $\mathbb{R}^2$ a $\mathbb{R}^3$, který jsme uvedli už dříve. Bez jakýchkoli tajemství nyní prozrazujeme, že tato podobnost není vůbec náhodná.

Věta 2.35. *Buď $\emptyset \neq M \subseteq V$, potom platí:*

(i) $\langle M \rangle \subset\subset V$.

(ii) $M \subset\subset V \Leftrightarrow M = \langle M \rangle$.

Důkaz. (i) Dokazujeme, že lineární obal neprázdné množiny je neprázdná množina, uzavřená na sčítání vektorů a násobení skalárem. Z předpokladu $M \neq \emptyset$ plyne $\langle M \rangle \neq \emptyset$. Zbývá ověřit, zda pro každé $x, y \in \langle M \rangle$ a $\alpha \in T$ platí $x + y \in \langle M \rangle$ a $\alpha x \in \langle M \rangle$. To už jsme ale dříve dokázali[38] v bodě (v) pozorování 2.32

[38] Respektive, dostali jsme za domácí úkol toto dokázat.

(ii) Musíme dokázat dvě implikace. Implikace ($\Leftarrow$) platí, neboť z předchozího bodu máme $\langle M \rangle \subset\subset V$, tedy $M = \langle M \rangle \subset\subset V$.

Dokážeme implikaci ($\Rightarrow$): Nechť M je podprostor, ověříme, že platí $M = \langle M \rangle$. Jelikož každá množina je podmnožinou svého vlastního lineárního obalu (opět pozorování 2.32), platí inkluze $M \subset \langle M \rangle$. Zbývá tedy dokázat inkluzi opačnou, $\langle M \rangle \subseteq M$:

Zvolme $x \in \langle M \rangle$, potom

$$x = \alpha_1 x_1 + \cdots + \alpha_n x_n \,,$$

pro nějaké $\alpha_i \in T, x_i \in M, i \in \hat{n}$. Protože M je podprostor, platí z uzavřenosti na násobení skalárem pro každý sčítanec $\alpha_i x_i \in M$ $(i \in \hat{n})$. Jejich součet pak leží v M díky uzavřenosti na sčítání. Platí tedy $x \in M$. □

Nyní už tedy víme, že v libovolném vektorovém prostoru platí: Všechny množiny uzavřené na „aplikaci lineárního obalu“ jsou právě všechny lineární obaly a to jsou právě všechny podprostory![39]

Se znalostí pojmu lineární obal a jeho vlastností můžeme konečně šikovněji formulovat alternativní charakterizaci vlastnosti LZ, a to že „soubor vektorů je LZ právě tehdy, pokud je jeden z vektorů souboru lineární kombinací ostatních“, a dokázat, že to je skutečně ekvivalentní vlastnost.

Věta 2.36. *Buď $(x_1, \dots, x_n)$ soubor vektorů z V a $n \geq 2$. Potom $(x_1, \dots, x_n)$ je LZ právě tehdy, když*

$$\exists k \in \hat{n} : x_k \in \langle x_1, \dots, x_{k-1}, x_{k+1}, \dots, x_n \rangle \,.$$

Důkaz. Dokážeme dvě implikace:

1. ($\Rightarrow$) : Je-li soubor $(x_1, \dots, x_n)$ LZ, existují $\alpha_1, \dots, \alpha_n \in T$ takové, že

$$\sum_{i=1}^{n} \alpha_i x_i = \theta$$

a přitom existuje index $k \in \hat{n}$, pro který $\alpha_k \neq 0$. Rovnici výše upravíme (odečteme sčítance $\alpha_i x_i$ pro $i \neq k$ a vydělíme nenulovým číslem[40] α_k) na[41]

$$x_k = \sum_{i \in \hat{n}, i \neq k} \Big(- \frac{\alpha_i}{\alpha_k} \Big) x_i \,,$$

což znamená, že $x_k \in \langle x_1, \dots, x_{k-1}, x_{k+1}, \dots, x_n \rangle$.

[39] A to se vědět vyplatí!

[40] Extrémně důležitá poznámka: zde násobíme inverzním prvkem k nenulovému α_k, což můžeme. Proč? Protože T je těleso!

[41] Netřeba se děsit sumy napravo – prostě sčítáme přes běžící index, který nabývá všech hodnot od 1 do n kromě k.

2. $(\Leftarrow)$: Je-li $x_k \in \langle x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n \rangle$, pak existují koeficienty $\beta_i \in T$ takové, že

$$x_k = \beta_1 x_1 + \ldots + \beta_{k-1} x_{k-1} + \beta_{k+1} x_{k+1} + \ldots + \beta_n x_n \,.$$

Odečteme-li x_k a dodefinujeme-li si $\beta_k := -1$, dostaneme

$$\sum_{i=1}^{n} \beta_i x_i = \theta \,,$$

tedy netriviální (alespoň $\beta_k \neq 0$) lineární kombinaci souboru $(x_1, \ldots, x_n)$ dávající nulový vektor, což znamená, že $(x_1, \ldots, x_n)$ je LZ. □

Z tohoto výsledku jde přímo odvodit jednoduchý důsledek, jehož důkaz ponecháváme na čtenářích: Je-li soubor vektorů LZ, lze z něj odebrat nějaký vektor a přitom nezměnit lineární obal souboru.

Důsledek 2.37. *Buď $(x_1, \ldots, x_n)$ LZ soubor vektorů z V, $n \geq 2$. Potom*

$$\exists k \in \hat{n} : \langle x_1, \ldots, x_n \rangle = \langle x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n \rangle \,.$$

V jistém smyslu „obrácené“[42] tvrzení nám říká, kdy lze LN soubor zvětšit a jeho nezávislost přitom zachovat.

Věta 2.38. *Buď $(x_1, \ldots, x_n)$ LN soubor vektorů z V a $y \notin \langle x_1, \ldots, x_n \rangle$. Potom soubor $(x_1, \ldots, x_n, y)$ je také LN.*

Důkaz. Zvolíme si libovolnou lineární kombinaci zvětšeného souboru. Předpokládejme, že pro nějakou volbu skalárů $\alpha_1, \alpha_2, \ldots, \alpha_{n+1} \in T$ platí

$$\alpha_1 x_1 + \ldots + \alpha_n x_n + \alpha_{n+1} y = \theta \,.$$

Dokážeme, že tato lineární kombinace musí být triviální. Uvažujme dva případy:

1. Je-li $\alpha_{n+1} = 0$, pak se jedná o lineární kombinaci pouze prvků z původního souboru $(x_1, \ldots, x_n)$. Ten je ovšem LN, tedy $\alpha_i = 0$ pro každé $i \in \widehat{n+1}$.

2. Nechť $\alpha_{n+1} \neq 0$, v rovnici výše pak lze číslem α_{n+1} dělit[43] a po zřejmých úpravách dostáváme

$$y = -\frac{\alpha_1}{\alpha_{n+1}} x_1 - \ldots - \frac{\alpha_n}{\alpha_{n+1}} x_n \,,$$

což je spor s předpokladem $y \notin \langle x_1, \ldots, x_n \rangle$. Situace $\alpha_{n+1} \neq 0$ tedy nikdy nenastává. Musí tedy $\alpha_{n+1} = 0$ a zbytek plyne z 1. bodu. □

Na závěr této podkapitoly zformulujeme často používané tvrzení dávající do souvislosti maticové násobení a lineární kombinace.

[42] Což je jen vágní a nijak nedefinovaný pojem.
[43] Opět si láskyplně vzpomeneme na axiomy tělesa...

Věta 2.39. *Mějme matice $\mathbb{A} \in T^{m,n}$ a $\mathbb{B} \in T^{n,k}$. Potom sloupce matice $\mathbb{AB}$ jsou lineárními kombinacemi souboru sloupců matice $\mathbb{A}$ a řádky matice $\mathbb{AB}$ jsou lineární kombinací souboru řádků matice $\mathbb{B}$.*

Důkaz. Ukažme tvrzení o sloupcích. Druhé tvrzení o řádcích se ukáže naprosto analogicky.

Pro každé $i \in \hat{m}$ a $j \in \hat{k}$ dle definice maticového násobení platí

$$(\mathbb{AB})_{ij} = \sum_{\ell=1}^{n} \mathbb{A}_{i\ell}\mathbb{B}_{\ell j}$$

a proto pro každé $j \in \hat{k}$ je

$$(\mathbb{AB})_{:j} = \sum_{\ell=1}^{n} \mathbb{B}_{\ell j}\mathbb{A}_{:\ell}.$$

Tedy $j$tý sloupec matice $\mathbb{AB}$ je lineární kombinací sloupců matice $\mathbb{A}$. $\square$

2.6 Báze a dimenze

V této části si představíme dva klíčové pojmy – *bázi* vektorového prostoru a jeho *dimenzi*. Ačkoli spolu intenzivně souvisí, oba si je zadefinujeme zvlášť.

Pojem báze si lze nejsnáze ilustrovat v jednoduchém vektorovém prostoru, v $\mathbb{R}^2$. Jeden z mnoha[44] příkladů báze je soubor $B = ((1,0),(0,1))$ dvou vektorů, z nichž každý určuje jednu ze dvou os kartézského souřadnicového systému. Tento soubor je tzv. bází $\mathbb{R}^2$ ze dvou důvodů. Jednak je „dost velký“[45] na to, aby šel každý jiný vektor z $\mathbb{R}^2$ vyjádřit jako lineární kombinace vektorů z B a jednak je lineárně nezávislý – tedy není „zbytečně velký“[46]. Další vlastnost bází, kterou oceníme především později při práci s lineárními zobrazeními, je ta, že namísto vektorů ve VP budeme moci pracovat pouze s jejich *souřadnicemi* v dané bázi – ať už je zvolena jakkoli.

O druhém stěžejním pojmu dimenze máme nejspíš každý nějakou intuitivní představu, rovině většinou přisuzujeme dimenzi 2 a „prostoru“ dimenzi 3. V obecném vektorovém prostoru V je to ale pojem abstraktnější, dimenze v jistém smyslu měří, jak je vektorový prostor V „velký“ – určuje, jaké největší lineárně nezávislé soubory lze ve V nalézt. Jak si mimo jiné spolu dokážeme, všechny báze daného vektorového prostoru mají počet prvků přesně rovný dimenzi.

Báze vektorového prostoru

Definice 2.40. *O množině vektorů M z vektorového prostoru V řekneme, že* ***generuje*** *prostor V, právě když platí:*

$$\langle M \rangle = V.$$

Definice 2.41. *Existuje-li ve V uspořádaná množina vektorů B taková, že*

[44] Jeden z nekonečně mnoha.
[45] Velmi lidově řečeno...
[46] Vzpomeňme na důsledek 2.37 o lineárně závislých souborech vektorů.

(i) B *je LN,*

(ii) B *generuje* V*,*

nazýváme B ***bází*** *vektorového prostoru* V*.*

Poznamenejme, že jeden vektorový prostor V může mít více různých bází – klidně i nekonečně mnoho! Nicméně, jak si později dokážeme, všechny báze jednoho prostoru musí mít stejný počet prvků. Před uvedením prvních příkladů bází si stručně shrňme, jak ověřit že daný soubor vektorů je bází vektorového prostoru.

Jelikož lineární nezávislost už ověřit umíme (viz algoritmus 2.27), zbývá umět ověřit druhou vlastnost bází a to, že generují celý prostor V. Z praktických důvodů se v algoritmu níže omezíme na ověřování u konečných souborů vektorů z V.

Algoritmus 2.42 (Ověření zda soubor generuje V)**.** *Pro zadaný soubor vektorů* $M = (x_1, \ldots, x_n)$ *ve vektorovém prostoru* V *ověřte, zda generuje celý VP.*

1. *Hledáme, jestli pro libovolný vektor* $v \in V$ *existuje nějaká ntice koeficientů* $\alpha_1, \ldots, \alpha_n \in T$ *taková, že příslušná lineární kombinace je rovna vektoru* v*.*

2. *Koeficienty* $\alpha_1, \ldots, \alpha_n \in T$ *považujme za neznámé v rovnici*

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = v.$$

3. *Z definice vektorových operací rovnici výše převeďme na soustavu lineárních rovnic (přesný postup závisí na konkrétní volbě prostoru* $(V, T, +, \cdot)$*). Vektor* v *nám pak do této soustavy (do její pravé strany) vnese nějaké parametry z* T*.*

4. *Soustavu převeďme pomocí GEM do horního stupňovitého tvaru. Dle věty 1.28 určeme, kolik existuje řešení.*

5. *Existuje-li pro libovolné hodnoty parametrů (tj. pro libovolný vektor* v*) alespoň jedno řešení, zadaný soubor generuje prostor* V*.*

Jak si můžeme snadno povšimnout, algoritmy 2.27 a 2.42 jsou si velice podobné. Stačí si uvědomit, že když z rovnic v bodech 2. obou algoritmů sestavujeme soustavy rovnic a ty následně řešíme pomocí GEM, tyto soustavy mají, až na pravé strany, stejné matice. Stačí tedy s touto soustavou pracovat jen jednou, a to s pravou stranou odvozenou z obecného vektoru $v \in V$. Z horního stupňovitého tvaru pak můžeme diskutovat obě vlastnosti bází najednou:

(i) Má-li soustava pro libovolnou pravou stranu alespoň jedno řešení, soubor generuje V.

(ii) Má-li přidružená homogenní soustava pouze jedno řešení, je soubor LN.[47]

Postup ilustrujeme na příkladech souborů z příkladů 2.28 a 2.29, pouze místo lineární nezávislosti zkoumáme druhou vlastnost bází.

[47] Přemýšlivý student jistě snadno dojde k podmínce, v jakém tvaru musí matice soustavy být, aby byl zkoumaný soubor bází – vzpomeňme na pozorování 1.23.

Příklad 2.43. *Ověříme, zda soubor* $((1,2,3),(4,7,8),(3,4,2)$ *generuje* $\mathbb{R}^3$.

Pro libovolný vektor $v=(v_1,v_2,v_3)\in\mathbb{R}^3$ *hledáme koeficienty* $\alpha,\beta,\gamma\in\mathbb{R}$ *takové, že platí*

$$\alpha(1,2,3)+\beta(4,7,8)+\gamma(3,4,2)=v=(v_1,v_2,v_3)\,.$$

Z definice vektorových operací pak dostáváme rovnost dvou vektorů z $\mathbb{R}^3$,

$$(\alpha+4\beta+3\gamma,2\alpha+7\beta+4\gamma,3\alpha+8\beta+2\gamma)=(v_1,v_2,v_3)\,,$$

která vede na soustavu lineárních rovnic v proměnných $\alpha,\beta,\gamma\in\mathbb{R}$.

Úpravou pomocí GEM pak dostáváme

$$\left(\begin{array}{ccc|c}1&4&3&v_1\\2&7&4&v_2\\3&8&2&v_3\end{array}\right)\sim\left(\begin{array}{ccc|c}1&4&3&v_1\\0&-1&-2&v_2-2v_1\\0&-4&-7&v_3-3v_1\end{array}\right)\sim\left(\begin{array}{ccc|c}1&4&3&v_1\\0&1&2&2v_1-v_2\\0&0&1&5v_1-4v_2+v_3\end{array}\right).$$

Jelikož se jedná o soustavu, jejíž rozšířená matice má jediný vedlejší sloupec (ten pravých stran), existuje pro každou trojici parametrů (v_1,v_2,v_3) *nějaké řešení* (α,β,γ) *a zadaný soubor generuje* $\mathbb{R}^3$. *Dokonce existuje vždy právě jedno řešení (tedy i pro nulovou pravou stranu, které odpovídá řešení* $(\alpha,\beta,\gamma)=(0,0,0)$*) a rovnou potvrzujeme i lineární nezávislost zadaného souboru – jedná se o bázi* $\mathbb{R}^3$.

Příklad 2.44. *Ověříme, zda soubor*

$$\left(\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}0&2\\0&1\end{pmatrix},\begin{pmatrix}1&0\\1&2\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix}\right)\quad \textit{generuje } \mathbb{Z}_3^{2,2}.$$

Pro libovolný vektor $v=\begin{pmatrix}v_{11}&v_{12}\\v_{21}&v_{22}\end{pmatrix}\in\mathbb{Z}_3^{2,2}$ *hledáme koeficienty* $\alpha,\beta,\gamma,\delta\in\mathbb{Z}_3=\{0,1,2\}$ *takové, že platí*

$$\alpha\begin{pmatrix}1&0\\1&1\end{pmatrix}+\beta\begin{pmatrix}0&2\\0&1\end{pmatrix}+\gamma\begin{pmatrix}1&0\\1&2\end{pmatrix}+\delta\begin{pmatrix}0&1\\0&0\end{pmatrix}=v=\begin{pmatrix}v_{11}&v_{12}\\v_{21}&v_{22}\end{pmatrix}.$$

Z definice vektorových operací pak dostáváme rovnost dvou vektorů z $\mathbb{Z}_3^{2,2}$,

$$\begin{pmatrix}\alpha+\gamma&2\beta+\delta\\\alpha+\gamma&\alpha+\beta+2\gamma\end{pmatrix}=\begin{pmatrix}v_{11}&v_{12}\\v_{21}&v_{22}\end{pmatrix},$$

která vede na soustavu lineárních rovnic v proměnných $\alpha,\beta,\gamma,\delta\in\mathbb{Z}_3$.

Úpravou pomocí GEM[48] *pak dostáváme*

$$\left(\begin{array}{cccc|c}1&0&1&0&v_{11}\\0&2&0&1&v_{12}\\1&0&1&0&v_{21}\\1&1&2&0&v_{22}\end{array}\right)\sim\left(\begin{array}{cccc|c}1&0&1&0&v_{11}\\0&2&0&1&v_{12}\\0&0&0&0&v_{21}+2v_{11}\\0&1&1&0&v_{22}+2v_{11}\end{array}\right)\sim\left(\begin{array}{cccc|c}1&0&1&0&v_{11}\\0&1&1&0&v_{22}+2v_{11}\\0&0&1&1&v_{12}+v_{22}+2v_{11}\\0&0&0&0&v_{21}+2v_{11}\end{array}\right).$$

Jelikož parametry $v_{11},v_{12},v_{21},v_{22}$ *volíme libovolně z* T, *existují volby, pro které má rozšířená matice soustavy poslední sloupec hlavní. Tedy existují vektory z* $\mathbb{Z}_3^{2,2}$, *které nejsou obsaženy v lineárním obalu zadaného souboru – ten tedy negeneruje celé* $\mathbb{Z}_3^{2,2}$ *a nemůže jít o bázi. Lineární závislost souboru bychom zjistili ze stejné matice, pro volbu* $v_{11}=v_{12}=v_{21}=v_{22}=0$ *zjevně existuje více než jedno řešení.*

[48] Pozor, pracujeme v $\mathbb{Z}_3$!

Příklad 2.45. *Nechť T je libovolné těleso s neutrálními prvky $0, 1$.*

- *Ve vektorovém prostoru T^n označme*

$$\begin{aligned} e_1 :=&(1, 0, 0, \dots, 0), \\ e_2 :=&(0, 1, 0, \dots, 0), \\ &\vdots \\ e_n :=&(0, 0, 0, \dots, 1). \end{aligned}$$

  Potom soubor $\mathcal{E}_n = (e_1, e_2, \dots, e_n)$ je báze T^n.

- *V prostoru $T^{m,n}$ lze zavést bázi analogicky. Soubor*

$$\mathcal{E}_{mn} = (e_{11}, \dots, e_{1n}, e_{21}, \dots, e_{2n}, \dots, e_{m1}, \dots, e_{mn}),$$

  kde e_{ij} je matice, která má na pozici s indexy ij jedničku a všude jinde nuly[49]*, je báze $T^{m,n}$.*

- *V prostoru T^∞ je situace s nalezením konkrétní báze trochu složitější. Nicméně, omezíme-li se na podprostor $P \subset\subset T^\infty$ obsahující všechny posloupnosti s konečně mnoha nenulovými členy, bázi snadno nalezneme. Označíme-li*

$$\begin{aligned} e_1 :=&(1, 0, 0, 0, \dots), \\ e_2 :=&(0, 1, 0, 0, \dots), \\ e_3 :=&(0, 0, 1, 0, \dots), \\ &\vdots \end{aligned}$$

  tedy pro každé $k \in \mathbb{N}$ je e_k nekonečná posloupnost nul s jedinou jedničkou na ké pozici. Potom nekonečná uspořádaná množina $\mathcal{E}_\infty = (e_1, e_2, e_3, \dots)$ je báze $P \subset\subset T^\infty$.

*Všechny báze v předchozích příkladech nazýváme **standardní báze** a značíme je jako výše, případně pouze $\mathcal{E}$ (bez indexace). U jejich prvků se můžeme často setkat s označením* jednotkové vektory.

Dimenze vektorového prostoru

Definice 2.46. *Buď V vektorový prostor nad T. Označme*

$$N_0(V) := \{n \in \mathbb{N}_0 \mid \textit{každý } (n+1)\textit{-členný soubor vektorů z } V \textit{ je LZ}\}$$

*Je-li $N_0(V) = \emptyset$, říkáme, že V **má nekonečnou dimenzi**, značíme*

$$\dim V = \infty.$$

*Je-li $N_0(V) \neq \emptyset$, říkáme, že V **má konečnou dimenzi** a definujeme*

$$\dim V = \min N_0(V).$$

[49] I zde rozumíme $0, 1 \in T$.

Příklad 2.47. *Uvažujme $V = \mathbb{R}^2$, v něm jistě existuje LN soubor délky 2, například $((1,0),(0,1))$. Současně víme, že každý soubor z $\mathbb{R}^2$ délky 3 (a tedy i každý větší*[50]*) je lineárně závislý. Z definice dostáváme*

$$N_0(\mathbb{R}^2) = \{2,3,4,5,\dots\}$$

a tedy platí

$$\dim \mathbb{R}^2 = \min\{2,3,4,5,\dots\} = 2.$$

Podobně bychom v $\mathbb{R}^3$ zjistili, že

$$N_0(\mathbb{R}^3) = \{3,4,5,\dots\}$$

a tedy

$$\dim \mathbb{R}^3 = \min\{3,4,5,\dots\} = 3.$$

Vášnivý čtenář jiných textů o lineární algebře by zde mohl namítnout, že naše definice dimenze je, lidově řečeno, „nějaká podivná“ – že on[51] zná definici jinou a jednodušší. Konkrétně: *Dimenze vektorového prostoru je počet prvků jeho báze.* Toto tvrzení je pravdivé a i my si ho v této části textu dokážeme. Jde o klasické dilema, kdy jeden pojem lze jednoznačně charakterizovat více vlastnostmi, které jsou ekvivalentní – jednu si musíme vybrat a ty další z ní dokázat. Přirozená otázka zní, proč je „naše“ definice lepší, resp. proč jsme ji vybrali. Je sice hůře představitelná, ale je logicky mnohem úspornější[52], jediné co k ní totiž potřebujeme je definice lineární (ne)závislosti! Naproti tomu *alternativní definice* výše potřebuje ke své smysluplnosti nejen znalost pojmu báze, ale také toho, že každý vektorový prostor bázi má a že všechny báze jednoho VP mají stejně prvků – což není úplně triviální, všechno si to spolu postupně teprve dokážeme.

Začneme několika jednoduchými vlastnostmi, které by přímo z definice dimenze měl každý umět odvodit a dokázat.

Věta 2.48.

(i) $\dim V = 0 \Leftrightarrow V = \{\theta\}$.

(ii) Triviální prostor $\{\theta\}$ nemá bázi.

(iii) Buď $n \in \mathbb{N}$ a nechť ve V existuje n-členný LN soubor. Potom

$$\dim V \geq n.$$

(iv) Buď $n \in \mathbb{N}_0$[53] *a nechť je ve V každý $(n+1)$-členný soubor LZ. Potom*

$$\dim V \leq n.$$

[50] Skutečně, zopakujte si, co platí pro každý LZ soubor, do kterého přidáme další vektor.

[51] Či ona!

[52] Můžete si vyhledat termín Occamova břitva, jde o myšlenkově blízký pojem.

[53] V textu se držíme konvence, že množina $\mathbb{N}$ neobsahuje nulu. $\mathbb{N}_0$ pak značí všechna přirozená čísla s přidanou nulou.

Důkaz. 1. Je-li $\dim V = 0$, potom $0 \in N_0(V)$. Tedy každý jednočlenný soubor vektorů ve V je LZ, z čehož plyne, že každý vektor ve V je nutně nulový, nebo-li $V = \{\theta\}$. Je-li naopak $V = \{\theta\}$, pak $0 \in N_0(V)$ a tedy $\dim V = 0$.

2. V triviálním vektorovém prostoru neexistuje žádný LN soubor, tudíž $\{\theta\}$ nemůže mít bázi.

3. Existuje-li nčlenný LN soubor, musí $n-1 \notin N_0(V)$. Jelikož každá podmnožina LN množiny je také LN, platí i $0, 1, \ldots, n-2 \notin N_0(V)$. Tedy

$$\dim V = \min N_0(V) \geq n.$$

4. Je-li každý $(n+1)$členný soubor LZ, pak $n \in N_0(V)$ a tedy

$$\dim V = \min N_0(V) \leq n. \qquad \square$$

Vlastnosti báze

Jelikož v tomto textu nechceme zabíhat do temných koutů teorie množin, budeme zde rigorózně dokazovat tvrzení o bázích často pouze k vektorovým prostorům konečné dimenze. Chybějící životní pravdy pro nekonečně dimenzionální vektorové prostory uvedeme bez důkazu v závěrečné poznámce.

Stěžejním výsledkem, který budeme v následujících důkazech potřebovat je takzvané Steinitzovo lemma o výměně. Je poměrně technické, proto jeho důkaz nebudeme v kurzu BI-LIN vyžadovat.

Lemma 2.49 (Steinitzovo o výměně)**.** *Nechť $(x_1, \ldots, x_n)$ a $(y_1, \ldots, y_m)$ jsou soubory vektorů z V. Předpokládejme, že je soubor $(x_1, \ldots, x_n)$ LN a současně je generován souborem $(y_1, \ldots, y_m)$, tedy $\forall i \in \hat{n} : x_i \in \langle y_1, \ldots, y_m \rangle$. Potom platí:*

(i) $n \leq m$, tedy délka LN souboru nesmí převýšit počet jeho generátorů.

(ii) Existují navzájem různé indexy $i_1, i_2, \ldots, i_n \in \hat{m}$ takové, že

$$\langle y_1, \ldots, y_m \rangle = \langle x_1, \ldots, x_n, (y_i \mid i \in \hat{m} \setminus \{i_1, i_2, \ldots, i_n\}) \rangle.$$ [54]

Věta 2.50. *Nechť $\dim V = n \in \mathbb{N}$. Potom ve V existuje n-členná báze.*

Důkaz. Protože $\dim V = n$, je $n-1 \notin N_0(V)$, a tedy ve V existuje LN soubor délky n, který označme $(x_1, \ldots, x_n)$. Chceme dokázat, že tento LN soubor také generuje V.

Určitě platí, že $\langle x_1, \ldots, x_n \rangle \subseteq V$. Stačí proto dokázat opačnou inkluzi, $V \subseteq \langle x_1, \ldots, x_n \rangle$, budeme postupovat sporem. Kdyby existoval prvek $x_{n+1} \in V$ takový, že $x_{n+1} \notin \langle x_1, \ldots, x_n \rangle$, pak by zvětšený soubor $(x_1, \ldots, x_n, x_{n+1})$ byl LN, jak víme z věty 2.38. To by ale znamenalo, že $\dim V \geq n+1$, tedy spor. $\square$

[54] Tedy, je možné ze souboru generátorů odstranit až n vektorů (s indexy $i_1, \ldots, i_n$) a ty nahradit všemi prvky generovaného LN souboru – přitom nezměníme lineární obal. Matematickým zápisem se nesmíme nechat zaskočit – prostě do souboru všech vektorů x_j přidáváme soubor, ve kterém jsou všechny y_i s indexy mimo ty vyhazované.

Věta 2.51. *Nechť $n \in \mathbb{N}$ a nechť ve V existuje n-členná báze. Potom* $\dim V = n$*. Existuje-li ve V nekonečná báze, pak* $\dim V = \infty$*.*

Důkaz. Označme nčlennou bázi V jako $(y_1, \ldots, y_n)$. Víme, že existence $n$prvkového LN souboru implikuje $\dim V \geq n$. Kdyby $\dim V > n$, musel by z definice dimenze ve V existovat LN soubor délky $n + 1$, označme jej $(x_1, \ldots, x_{n+1})$. Platí ovšem

$$\forall i \in \{1, \ldots, n+1\} : x_i \in V = \langle y_1, \ldots, y_n \rangle \, ,$$

což je předpoklad Steinitzova lemmatu, podle kterého délka LN souboru nemůže převýšit počet generátorů, tj. musí platit $n + 1 \leq n$, což je spor.

Existuje-li ve V nekonečná báze, existují ve V LN soubory libovolné délky (libovolné konečné podmnožiny této báze). Proto $N_0(V) = \emptyset$ a podle definice dimenze je v takovém případě $\dim V = \infty$. □

Důsledek 2.52. *Všechny báze vektorového prostoru V mají stejný počet prvků, roven* $\dim V$*.*

Důkaz. Předpokládejme nejprve, že ve V existují dvě konečné báze, jedna s $m \in \mathbb{N}$ vektory a druhá s $n \in \mathbb{N}$ vektory. Podle předchozí věty potom $m = \dim V$ a současně $n = \dim V$. Dimenze V je ale jednoznačně určené číslo, a proto $m = n$.

Pokud by ve V existovala jedna konečná báze s $n \in \mathbb{N}$ vektory a jedna nekonečná báze, dostali bychom podobně jako v předchozím bodě aplikací předchozí věty, že $\dim V = n$ a současně $\dim V = \infty$. To je opět spor s jednoznačností dimenze VP. □

Už tedy víme, že v každém netriviálním vektorovém prostoru existuje báze, víme, kolik má mít prvků a také víme, jak ověřit, zda nějaký soubor nebo množina bází je. Co ale vlastně moc nevíme je, jak nějakou bázi konkrétně najít, případně vytvořit ze souborů, které bázemi nejsou. O tom budou následující dvě jednoduchá tvrzení. V obou případech budeme mít k dispozici nějaký soubor vektorů, který z vlastností báze splňuje právě jednu – a my si dokážeme, že lze vytvořit soubor, který splňuje obě.

Věta 2.53. *Nechť $\{\theta\} \neq V = \langle y_1, \ldots, y_n \rangle$. Potom* $\dim V = k \leq n$ *a existují navzájem různé indexy $i_1, \ldots, i_k \in \hat{n}$ takové, že $(y_{i_1}, \ldots, y_{i_k})$ je báze V.*

Jinými slovy: z každého generujícího souboru lze vybrat bázi.

Důkaz. První část tvrzení plyne ze Steinitzova lemmatu. Druhá část věty plyne z faktu, že v LZ souboru existuje prvek, který lze ze souboru odebrat, aniž by se změnil jeho lineární obal (viz důsledek 2.37).

Takto můžeme ze souboru $(y_1, \ldots, y_n)$ postupně odebírat prvky tak dlouho, dokud vzniklý soubor nebude LN. To nastane, až bude v souboru zbývat k vektorů, protože $\dim V = k$. □

Věta 2.54. *Nechť $(x_1, \ldots, x_k)$ je LN soubor vektorů z V a* $\dim V = n \in \mathbb{N}$*. Potom existují vektory $x_{k+1}, \ldots, x_n \in V$ takové, že $(x_1, \ldots, x_n)$ je báze V.*

Jinými slovy: každý lineárně nezávislý soubor lze doplnit na bázi.

Důkaz. Buď $(y_1, \dots, y_n)$ nějaká báze V. Ze Steinitzova lemmatu plyne, že $k \leq n$ a že existují navzájem různé indexy $i_1, i_2, \dots, i_k \in \hat{n}$ takové, že

$$V = \langle y_1, \dots, y_n \rangle = \langle x_1, \dots, x_k, (y_i \mid i \in \hat{n} \setminus \{i_1, i_2, \dots, i_k\}) \rangle.$$

Máme tedy nčlenný soubor generátorů obsahující vektory $x_1, \dots, x_k$.

Stačí si rozmyslet, že tento soubor je LN. Kdyby soubor $(x_1, \dots, x_k, (y_i \mid i \in \hat{n} \setminus \{i_1, i_2, \dots, i_k\}))$ byl LZ, můžeme z jeho vektorů vybrat LN soubor délky $\ell < n$ generující V, což je ale ve sporu s $\dim V = n$. □

Poznámka 2.55. *I když to v textu formálně nedokazujeme, důležitá tvrzení platí i pro prostory nekonečné dimenze:*

(i) I ve vektorovém prostoru o $\dim V = \infty$ existuje báze (nekonečná).

(ii) Z nekonečné množiny generátorů lze také vybrat bázi.

(iii) I ve vektorovém prostoru o $\dim V = \infty$ lze každý LN soubor doplnit na bázi.

Vlastnosti dimenze

Příklad 2.56. *Z existence standardních bází (příklad 2.45) lze rovnou vyvodit následující poznatky:*

- $\dim T^n = n$.
- $\dim T^{m,n} = mn$.
- $\dim T^\infty = \infty$.

Speciálně tedy platí $\dim(\mathbb{R}^n, \mathbb{R}, +, \cdot) = n$ a $\dim(\mathbb{C}^n, \mathbb{C}, +, \cdot) = n$, rozepíšeme-li explicitně, nad kterým tělesem pracujeme.

Zajímavým příkladem je ale prostor $(\mathbb{C}^n, \mathbb{R}, +, \cdot)$, tedy prostor ntic komplexních čísel nad tělesem reálných čísel – tedy vektory lze násobit pouze reálnými čísly. Zkuste si sami ověřit, že se skutečně jedná o VP a že navíc platí

$$\dim(\mathbb{C}^n, \mathbb{R}, +, \cdot) = 2n\,,$$

například tím, že naleznete nějakou bázi tohoto prostoru[55].

Základy pojmu podprostor už máme v malíčku, proto se nyní zaměříme na zkoumání, jak je to s jeho dimenzí v závislosti na dimenzi VP a dále pak co platí pro dimenze průniku a součtu podprostorů – jak máme dokázáno, výsledky obou operací jsou také podprostory, tedy má smysl bavit se o jejich dimenzi.

Věta 2.57. *Nechť V je VP a $P \subset\subset V$. Potom*

$$\dim P \leq \dim V.$$

Je-li navíc P vlastní podprostor V a $\dim V < \infty$, potom

$$\dim P < \dim V.$$

Důkaz. Je-li $\dim V = \infty$ první tvrzení věty platí triviálně[56].

[55] Pozor, následující část vyzrazuje zápletku nebo rozuzlení díla: Bázi můžeme zvolit podobně jako standardní, například $(1, 0, \dots, 0), (i, 0, \dots, 0), \dots, (0, \dots, 0, 1), (0, \dots, 0, i))$

[56] Jistě platí pro každé $n \in \mathbb{N}$, že $n \leq \infty$ a také $\infty \leq \infty$.

Nechť tedy $\dim V < \infty$ a $P \subset\subset V$. Potom platí $N_0(V) \subseteq N_0(P)$. Skutečně, platí-li $n \in N_0(V)$, pak jsou všechny $(n+1)$členné soubory z V LZ, pak jsou ale i všechny $(n+1)$členné soubory z P LZ (P je podmnožina V).

Současně nemůže být množina $N_0(P)$ prázdná. Kdyby byla, muselo by platit i $N_0(V) = \emptyset$ a nutně pak $\dim V = \infty$, to by byl spor.

Z inkluze $N_0(V) \subseteq N_0(P)$ nakonec tedy dostáváme

$$\dim P = \min N_0(P) \leq \min N_0(V) = \dim V\,.$$

Buď nyní $P \subset\subset V$ vlastní podprostor, tj. $P \neq V$, a nechť $\dim V = n < \infty$. Víme už, že $\dim P = k \leq n$, chceme dokázat ostrou nerovnost $k < n$. Je-li $\dim P = 0$, tj. $P = \{\theta\}$, musí $V \neq \{\theta\}$, a tedy $n = \dim V \geq 1$ a nerovnost platí. Je-li $\dim P = k \geq 1$, existuje báze P, označme ji $(x_1, \dots, x_k)$. Protože $P \neq V$, existuje $x_{k+1} \in V$ takový, že $x_{k+1} \notin P$, a tedy $(x_1, \dots, x_k, x_{k+1})$ je LN, odkud rovnou plyne $\dim V \geq k+1$. V obou případech platí $\dim P < \dim V$. $\square$

Potenciálně užitečný důsledek této věty nám pak říká, že pokud o nějakém podprostoru dokážeme, že má stejnou konečnou dimenzi jako celý vektorový prostor V, musí se mu nutně rovnat.

Důsledek 2.58. *Buď $P \subset\subset V$ a $\dim P = \dim V < \infty$. Potom $P = V$.*

Poznámka 2.59. *Předpoklad $\dim V < \infty$ v druhé části tvrzení věty 2.57 je podstatný. Ve vektorovém prostoru $\mathbb{C}^\infty$ nekonečných komplexních posloupností je například množina $M = \{(\alpha_1, \alpha_1, \alpha_2, \alpha_2, \alpha_3, \alpha_3, \dots) \mid \forall i \in \mathbb{N} : \alpha_i \in \mathbb{C}\}$ vlastním podprostorem a přitom platí*

$$\dim M = \dim \mathbb{C}^\infty = \infty.$$

Definice 2.60. *Bud V vektorový prostor a $\emptyset \neq A \subseteq V$, $\emptyset \neq B \subseteq V$. Součet $A + B$ nazveme **direktní**, právě když pro každý vektor $x \in A + B$ existuje jediné $a \in A$ a jediné $b \in B$ takové, že*

$$x = a + b\,.$$

Direktní součet značíme $A \oplus B$[57].

Příklad 2.61. *Stejně jako v příkladu 2.19, volme ve VP $\mathbb{R}^2$ dva podprostory:*

$$E_1 := \mathbb{R} \times \{0\}\,, \quad E_2 := \{0\} \times \mathbb{R}\,.$$

Už víme, že platí $E_1 + E_2 = \mathbb{R}^2$, dokonce ale platí i

$$E_1 \oplus E_2 = \mathbb{R}^2\,.$$ [58]

Na druhou stranu, ve VP $\mathbb{R}^3$ následující součet

$$\langle (1,0,0), (0,1,0) \rangle + \langle (1,0,0), (0,0,1) \rangle = \mathbb{R}^3$$

*direktní **není**.*

[57] Což si samozřejmě nebudeme plést s explicitně zdůrazněnou operací sčítání vektorů – jistě rozeznáme vektor od množiny.

[58] Nad tímhle se zkuste férově zamyslet.

V případě, že P, Q jsou podprostory, si lze direktnost jejich součtu snáze představit pomocí ekvivalentní vlastnosti *mít triviální průnik*, jak říká další věta.

Věta 2.62. *Buďte $P \subset\subset V$, $Q \subset\subset V$. Potom $P + Q$ je direktní právě tehdy, když*

$$P \cap Q = \{\theta\}.$$

Důkaz. $(\Rightarrow)$: Nechť $P + Q$ je direktní. Kdyby $P \cap Q \neq \{\theta\}$, existoval by nenulový prvek $a \in P \cap Q$ a tedy $a \in P$ a $a \in Q$. Jelikož podprostor je uzavřený na násobení skalárem, platilo by i $-a \in Q$. Tedy nulový vektor $\theta \in P + Q$ by šel rozložit na součet dvou vektorů z P a Q dvěma způsoby:

$$\theta = \theta + \theta = a + (-a),$$

což by byl spor s direktností součtu $P + Q$.

$(\Leftarrow)$: Nechť $P \cap Q = \{\theta\}$ a pro spor předpokládejme, že $P + Q$ není direktní. Existuje tedy $x \in P + Q$ takové, že

$$x = \underbrace{a_1}_{\in P} + \underbrace{b_1}_{\in Q} = \underbrace{a_2}_{\in P} + \underbrace{b_2}_{\in Q},$$

kde $a_1 \neq a_2$ a $b_1 \neq b_2$. Potom ovšem platí

$$\theta \neq \underbrace{a_1 - a_2}_{\in P} = \underbrace{b_2 - b_1}_{\in Q}$$

a v průniku $P \cap Q$ se tak nachází nenulový vektor $a_1 - a_2$, což je spor. □

Důležitou souvislost mezi dimenzemi podprostorů, jejich průniků a součtů dává 1. věta o dimenzi. Její důkaz si pro větší rozsah neuvedeme a nebudeme jej ani vyžadovat.

Věta 2.63 (1. o dimenzi)**.** *Buďte $P, Q \subset\subset V$. Potom platí:*

$$\dim(P + Q) + \dim(P \cap Q) = \dim P + \dim Q,$$

speciálně pro direktní součet platí:

$$\dim(P \oplus Q) = \dim P + \dim Q.$$

Jak už jsme si řekli, každý vektorový prostor (potažmo i každý podprostor) může mít více bází. Tedy úlohy typu *nalezněte bázi zadaného podprostoru* nemají jednoznačné řešení. Chceme-li pak porovnat správnost dvou různých výsledků, jde v podstatě o ověření, zda dva různé soubory vektorů generují stejný (pod)prostor, tedy zda se rovnají jejich lineární obaly. K tomu se nám v budoucnu bude hodit následující pozorování, využívající pojem dimenze[59].

[59]Bohužel až budoucnu. Zatím totiž nemáme k dispozici jednoduché pravidlo pro výpočet dimenze lineárního obalu zadaného souboru vektorů. K tomu se nám bude hodit pojem *hodnost matice*, který si zavedeme v následující kapitole!

Pozorování 2.64. *Buďte* $(x_1, \ldots, x_n)$ *a* $(y_1, \ldots, y_m)$ *dva soubory vektorů z* V. *Potom*

$$\langle x_1, \ldots, x_n \rangle = \langle y_1, \ldots, y_m \rangle$$

právě tehdy, když

$$\dim\langle x_1, \ldots, x_n \rangle = \dim\langle y_1, \ldots, y_m \rangle = \dim\langle x_1, \ldots, x_n, y_1, \ldots, y_m \rangle.$$

Důkaz. $(\Rightarrow)$: Z rovnosti $\langle x_1, \ldots, x_n \rangle = \langle y_1, \ldots, y_m \rangle$ speciálně máme

$$\forall j \in \hat{m} : y_j \in \langle x_1, \ldots, x_n \rangle.$$

Proto přidáním vektorů $y_1, \ldots, y_m$ do souboru $(x_1, \ldots, x_n)$ se nezmění obal souboru. Je tedy

$$\langle x_1, \ldots, x_n \rangle = \langle x_1, \ldots, x_n, y_1, \ldots, y_m \rangle\,.$$

Všechny tři obaly se rovnají, a proto musejí mít také stejnou dimenzi.
$(\Leftarrow)$: Naopak, protože

$$\langle x_1, \ldots, x_n \rangle \subset\subset \langle x_1, \ldots, x_n, y_1, \ldots, y_m \rangle$$

a dimenze obou obalů se rovnají (dle předpokladu), musejí se už oba tyto prostory rovnat, podle důsledku 2.58. Stejnou úvahou dojdeme i k rovnosti

$$\langle y_1, \ldots, y_m \rangle = \langle x_1, \ldots, x_n, y_1, \ldots, y_m \rangle\,.$$

Celkem proto platí $\langle x_1, \ldots, x_n \rangle = \langle y_1, \ldots, y_m \rangle$. □

Souřadnice vektoru v bázi

Poznámka 2.65. *Budeme-li chtít v následujícím textu explicitně zdůraznit, že uvažovaný vektorový prostor* V *má dimenzi* n, *a přitom šetřit místem, budeme jej značit* V_n.

Věta 2.66. *Nechť* $\mathcal{X} = (x_1, \ldots, x_n)$ *je báze* V_n. *Potom ke každému* $z \in V_n$ ***existuje právě jedna*** *uspořádaná ntice* $(\alpha_1, \ldots, \alpha_n) \in T^n$ *taková, že*

$$z = \sum_{i=1}^{n} \alpha_i x_i.$$

Důkaz. Existence $(\alpha_1, \ldots, \alpha_n)$: Protože báze generuje VP, neboli $V_n = \langle x_1, \ldots, x_n \rangle$, musí existovat čísla $\alpha_1, \ldots, \alpha_n \in T$ (koeficienty lineární kombinace) taková, že

$$z = \sum_{i=1}^{n} \alpha_i x_i.$$

Jednoznačnost: Pro spor předpokládejme, že existuje nějaká další $n$tice koeficientů $(\beta_1, \ldots, \beta_n) \in T^n$ taková, že $\exists i \in \hat{n} : \alpha_i \neq \beta_i$ a

$$z = \sum_{i=1}^{n} \alpha_i x_i = \sum_{i=1}^{n} \beta_i x_i\,.$$

Potom nutně[60] platí také

$$\sum_{i=1}^{n}(\alpha_i - \beta_i)x_i = \theta.$$

Soubor $(x_1, \ldots, x_n)$ je ovšem LN, tedy nulový vektor lze získat pouze triviální lineární kombinací a nutně $\forall i \in \hat{n} : \alpha_i - \beta_i = 0$, což je spor. □

Definice 2.67. *Nechť $\mathcal{X} = (x_1, \ldots, x_n)$ je báze V_n a vektor $z \in V_n$ splňuje*

$$z = \sum_{i=1}^{n} \alpha_i x_i \,.$$

*Číslo $\alpha_i \in T$ nazýváme i-tá **souřadnice vektoru z v bázi $\mathcal{X}$**.*

Dále pro $\forall i \in \hat{n}$ zavedeme zobrazení $x_i^{\#} : V_n \to T$ vztahem

$$x_i^{\#}(z) := \alpha_i.$$

*Toto zobrazení nazýváme i-tý **souřadnicový funkcionál v bázi $\mathcal{X}$**.*

Zdůrazněme, že oba pojmy *souřadnice v bázi* a *souřadnicový funkcionál v bázi* jsou opravdu korektně definovány. I když tím jen opakujeme důkaz věty 2.66, je užitečné ještě jednou poznamenat, že právě existence a jednoznačnost souřadnic je ta hlavní motivace, proč se báze definuje tak, jak se definuje. Obě vlastnosti bází jsou potřeba!

(i) Díky tomu, že báze generuje V_n, souřadnice $x_i^{\#}(z) = \alpha_i$ vůbec existují.

(ii) Díky lineární nezávislosti báze jsou navíc určeny jednoznačně.

Jak můžeme nalézt souřadnice zadaného vektoru v nějaké bázi? Využijeme a jen lehce upravíme postup v algoritmu 2.42:

Algoritmus 2.68 (Nalezení souřadnic vektoru v bázi)**.** *Pro zadaný vektor $z \in V$ a bázi $\mathcal{X} = (x_1, \ldots, x_n)$ vektorového prostoru V_n nalezněte souřadnice z v bázi $\mathcal{X}$.*

1. *Hledáme ntici koeficientů $\alpha_1, \ldots, \alpha_n \in T$ takovou, že příslušná lineární kombinace prvků báze je rovna vektoru z.*

2. *Koeficienty $\alpha_1, \ldots, \alpha_n \in T$ považujme za neznámé v rovnici*

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = z \,.$$

3. *Z definice vektorových operací rovnici výše převeďme na soustavu lineárních rovnic (přesný postup závisí na konkrétní volbě prostoru $(V_n, T, +, \cdot)$). Pravá strana soustavy bude určena vektorem z.*

4. *Soustavu převeďme pomocí GEM do horního stupňovitého tvaru. Jelikož $\mathcal{X} = (x_1, \ldots, x_n)$ je báze, musí existovat právě jedno řešení $(\alpha_1, \ldots, \alpha_n)$ této soustavy – a to jsou hledané souřadnice vektoru z v bázi $\mathcal{X}$.*

[60] Proč nutně? Nechť se každý zamyslí nad tím, jaké axiomy a jejich důsledky jsme k provedeným úpravám vlastně potřebovali…

Příklad 2.69. *Ve standardní bázi* $\mathcal{E}_3 = (e_1, e_2, e_3)$ *prostoru* $\mathbb{R}^3$ *má vektor* $z = (a, b, c)$ *souřadnice* (a, b, c). *Skutečně, triviálně platí* $(a, b, c) = a(1, 0, 0)+b(0, 1, 0)+c(0, 0, 1)$, *tedy*

$$z = ae_1 + be_2 + ce_3 \,.$$

Pro jednotlivé souřadnicové funkcionály máme:

$$e_1^{\#}(z) = a, \qquad e_2^{\#}(z) = b, \qquad e_3^{\#}(z) = c\,.$$

Příklad 2.70. *Soubor* $\mathcal{X} = (x_1, x_2, x_3)$, *kde*

$$x_1 = (1, 1, 1), \quad x_2 = (1, 1, 2), \quad x_3 = (1, 2, 3),$$

je jiná báze $\mathbb{R}^3$. *Souřadnice vektoru* $z = (a, b, c)$ *nalezneme dle algoritmu 2.68.*

Řešíme rovnici

$$\alpha(1, 1, 1) + \beta(1, 1, 2) + \gamma(1, 2, 3) = z = (a, b, c)\,,$$

s parametry $a, b, c \in \mathbb{R}$ *a neznámými* $\alpha, \beta, \gamma \in \mathbb{R}$ *Přímo získanou SLR řešíme Gaussovou eliminací*[61]*:*

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & a \\ 1 & 1 & 2 & b \\ 1 & 2 & 3 & c \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & 1 & a \\ 0 & 0 & 1 & b-a \\ 0 & 1 & 2 & c-a \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & 1 & a \\ 0 & 1 & 2 & c-a \\ 0 & 0 & 1 & b-a \end{array}\right) \sim$$
$$\sim \left(\begin{array}{ccc|c} 1 & 1 & 0 & 2a-b \\ 0 & 1 & 0 & a-2b+c \\ 0 & 0 & 1 & b-a \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 0 & a+b-c \\ 0 & 1 & 0 & a-2b+c \\ 0 & 0 & 1 & b-a \end{array}\right),$$

s výsledkem $(\alpha, \beta, \gamma) = (a + b - c, a - 2b + c, b - a)$. *Tedy*

$$z = (a + b - c)x_1 + (a - 2b + c)x_2 + (-a + b)x_3$$

a pro jednotlivé souřadnicové funkcionály nyní máme

$$x_1^{\#}(z) = a + b - c, \qquad x_2^{\#}(z) = a - 2b + c, \qquad x_3^{\#}(z) = -a + b.$$

Poznámka 2.71. *V dalším textu budeme s oblibou pro zkrácení zápisů používat praktický symbol,* ***Kroneckerovo delta****, definovaný předpisem:*

$$\delta_{ij} = \begin{cases} 1, & \text{pro } i = j, \\ 0, & \text{jinak.} \end{cases}$$

Zavedením souřadnicových funkcionálů pro mnoho studentů dojde na takzvané lámání chleba. Je třeba vytrvat a symbolu $x_i^{\#}(z)$ se nezaleknout – je to prostě jen matematický zápis pro i-tou souřadnici vektoru z v bázi $(x_1, \dots, x_n)$. Jedná se rozhodně o praktičtější označení než *„koeficient u i-tého prvku báze při vyjádření vektoru z jako lineární kombinace prvků báze“*[62]. Je třeba jen správně rozlišovat symboly a mít naprosto jasno v několika důležitých faktech:

[61] Poznamenejme, že už v třetím kroku bychom mohli s úpravami skončit, soustava je v horním stupňovitém (dokonce trojúhelníkovém) tvaru! Protože to ovšem daná soustava umožňuje, můžeme ji ještě několika snadnými úpravami dále zjednodušovat.

[62] No, uznejte sami, že opravdu je.

- $x_i^\#$ je zobrazení $V_n \to T$. Na vstupu přijme libovolný vektor a přiřadí mu takové číslo z tělesa, které při vyjádření tohoto vektoru lineární kombinací „stojí“ před $i$tým bazickým vektorem.
- $x_i^\#(z)$ je číslo, prvek z tělesa T! Tedy koeficient v lineární kombinaci konkrétního vektoru z, v textu výše typicky značený α_i[63].
- Uvidíme-li někde napsáno
$$z = \sum_{i=1}^{n} x_i^\#(z) x_i$$
pro nějaký vektor $z \in V_n$ a bázi $\mathcal{X} = (x_1, \dots, x_n)$, je to tentýž zápis lineární kombinací bazických vektorů jako
$$z = \sum_{i=1}^{n} \alpha_i x_i\,,$$
pouze je explicitně vyznačena použitá báze.
- Připomeňme, že pro j-tou složku i-tého vektoru e_i standardní báze prostoru T^n platí:
$$(e_i)_j = \delta_{ij}.$$
- Tedy, ve standardní bázi $\mathcal{E}_n = (e_1, \dots, e_n)$ prostoru T^n má každý vektor $z = (\alpha_1, \dots, \alpha_n)$ souřadnice $(\alpha_1, \dots, \alpha_n)$, neboť[64]
$$z = \sum_{i=1}^{n} \alpha_i e_i.$$

Věta 2.72. *Nechť $i \in \hat{n}$ a $x_i^\# : V_n \to T$ je i-tý souřadnicový funkcionál v bázi $(x_1, \dots, x_n)$. Potom platí:*

(i) $\forall x, y \in V_n : x_i^\#(x + y) = x_i^\#(x) + x_i^\#(y)$,

(ii) $\forall x \in V_n,\ \forall \alpha \in T : x_i^\#(\alpha x) = \alpha x_i^\#(x)$,

(iii) $\forall j \in \hat{n} : x_i^\#(x_j) = \delta_{ij}$.

Důkaz. (i) Nechť $x, y \in V_n$. Máme tedy
$$x = \sum_{i=1}^{n} x_i^\#(x) x_i\,, \qquad y = \sum_{i=1}^{n} x_i^\#(y) x_i\,.$$

Odtud rovnou plyne
$$x + y = \sum_{i=1}^{n} x_i^\#(x) x_i + \sum_{i=1}^{n} x_i^\#(y) x_i = \sum_{i=1}^{n} \Big(x_i^\#(x) + x_i^\#(y) \Big) x_i.$$

[63] Dříve jsme holt nepotřebovali značením rozlišovat různé báze.

[64] Tedy standardní báze je přesně taková, jako bychom od slova standardní čekali – souřadnice každého vektoru v ní jsou stejné, jako když tento vektor napíšeme „tak, jak je“.

Současně je $x + y \in V_n$ a musí tedy platit

$$x + y = \sum_{i=1}^{n} x_i^{\#}(x + y) x_i \,.$$

Protože souřadnice jsou určeny jednoznačně (viz předchozí věta), získáváme

$$\forall i \in \hat{n} : x_i^{\#}(x + y) = x_i^{\#}(x) + x_i^{\#}(y).$$

(ii) Pozorný čtenář si snadno dokáže analogicky ke kroku (i).

(iii) Zapíšeme-li vektor x_j jako[65]

$$x_j = \sum_{i=1}^{n} \delta_{ij} x_i,$$

dostaneme opět z jednoznačnosti souřadnic, že $x_i^{\#}(x_j) = \delta_{ij}$. $\square$

[65] Zkuste si sumu rozepsat bez symbolu δ_{ij}, mělo by to jít rovnou vidět.

Kapitola 3

Hodnost matice a Frobeniova věta

Hlavním cílem této kapitoly je konečně si vysvětlit, jak to přesně je s řešením soustav lineárních rovnic. O jejich řešitelnosti už základní věci víme, máme v malíčku Gaussovu eliminační metodu (GEM) a z horního stupňovitého tvaru soustavy poznáme, zda je soustava řešitelná, případně jestli má více než jedno řešení. Krom toho ještě víme, jak množina řešení S souvisí s množinou řešení S_0 přidružené homogenní soustavy a jak **nějaká** řešení najít.

Zatím jsme ale neměli k dispozici žádné precizně formulované tvrzení o tom, jak přesně vypadá množina **všech** řešení – to se změní s vyslovením Frobeniovy věty! Takový pokrok samozřejmě nemůže být zadarmo, my si ho zasloužíme definováním několika nových pojmů, jako například *hodnost matice*, *regulární matice* nebo *inverzní matice*, a odvozením dalších vlastností maticového násobení. Výsledkem našeho snažení pak nebude „jen“ popis řešení soustav, jako vedlejší produkt zkoumání hodností matic si odvodíme i praktická pravidla pro řešení několika typů úloh s lineárními obaly v prostorech T^n. Ukážeme si také trochu odlišný pohled na GEM, a to s pomocí maticového násobení. Tato interpretace povede k jednoduchému algoritmu na hledání inverzí zadaných matic a ověření jejich regularity.

Na své si v celé této kapitole dozajista přijdou hlavně věční pochybovači o užitečnosti lineární algebry. Skutečně, ať už půjde o algoritmický návod k hledání všech řešení soustavy lineárních rovnic, o důkaz, že známe opravdu všechna řešení, nebo o způsob, jak množinu řešení konečně inteligentně zapsat, konečně při tom naplno využijeme doposud zavedené pojmy a vyloženou teorii!

3.1 Co si z této kapitoly odneseme

1. Seznámíme se s pojmem hodnost matice a ukážeme, jak ji snadno určit pomocí GEM

2. Zavedeme novou maticovou operaci, *inverzi*. Matice, které inverzi mají, nazveme *regulární* a regularitu matice dáme do souvislosti s její hodností.

3. Odvodíme si, že celá GEM v podstatě spočívá jen v opakovaném násobení matice soustavy vhodnými regulárními maticemi! Naučíme se, jak regularitu matic ověřovat a jak hledat jejich inverze.

4. Vyložíme si rigorózní postup, jak nalézt všechna řešení SLR a jak je elegantním způsobem zapsat.

5. Množiny všech řešení SLR geometricky interpretujeme, a to pojmem lineární varieta.

3.2 Hodnost matice

Definice 3.1. *Nechť $\mathbb{A}, \mathbb{B} \in T^{m,n}$. Je-li možné matici $\mathbb{A}$ převést konečně mnoha řádkovými úpravami (G1)-(G3) Gaussovy eliminační metody na matici $\mathbb{B}$, budeme tuto skutečnost zkráceně zapisovat*

$$\mathbb{A} \sim \mathbb{B}\,.$$

Po krátkém zamyšlení jistě odvodíme, že každý z kroků GEM je vratný[1], tedy platí $\mathbb{A} \sim \mathbb{B} \Rightarrow \mathbb{B} \sim \mathbb{A}$. Současně musíme zdůraznit jeden důležitý fakt. Zatímco při samotném řešení soustav lineárních rovnic je někdy možné „ignorovat“[2] nulové řádky a množinu řešení to nezmění, *odstranění nulového řádku* formálně **nepatří** mezi základní kroky Gaussovy eliminační metody! Proto vztah $\sim$ definujeme pouze pro matice stejných rozměrů.

Definice 3.2. *Nechť $\mathbb{A} \in T^{m,n}$. **Hodností matice** $\mathbb{A}$ nazýváme dimenzi lineárního obalu souboru řádků matice $\mathbb{A}$ (jako vektorů z $T^{1,n}$) a značíme ji $h(\mathbb{A})$. Tedy:*

$$h(\mathbb{A}) = \dim\langle \mathbb{A}_{1:}, \ldots, \mathbb{A}_{m:}\rangle.$$

Poznamenejme, že přímo z definice vyplývá omezení $h(\mathbb{A}) \leq m$ pro každou matici $\mathbb{A}$ typu $m \times n$. Z vlastností lineárních obalů pak jistě pozorný čtenář odvodí následující pozorování.

Pozorování 3.3. *Nechť $\mathbb{A}, \mathbb{B} \in T^{m,n}$ a $\mathbb{A} \sim \mathbb{B}$, potom*

$$\langle \mathbb{A}_{1:}, \ldots, \mathbb{A}_{m:}\rangle = \langle \mathbb{B}_{1:}, \ldots, \mathbb{B}_{m:}\rangle.$$

Tedy aplikace elementárních kroků GEM nijak nemění lineární obal souboru řádků matice. I když to zde nebudeme podrobně rozepisovat, skutečně se sami zamyslete nad tím, jak se změní lineární obal souboru vektorů, se kterým provedeme úpravy odpovídající (G1)–(G3)[3]. Přímým důsledkem tohoto pozorování[4] je pak následující věta, která říká, že Gaussova eliminace **nemění hodnost** upravované matice. Následujícím tvrzením pak vysvětlíme jak snadno určit hodnost matice v horním stupňovitém tvaru.

---

[1] Zkuste sami formulovat ke každé úpravě (G1)–(G3) takovou úpravu, která vede zpátky k původní matici.

[2] Tedy je prostě přestat psát.

[3] Vlastně můžeme ignorovat fakt, že se jedná o řádky nějaké matice. Jedná se o soubor $n$tic, vektorů z $T^{1,n}$, u kterých můžeme prohodit pořadí, násobit vektor nenulovým číslem a nahradit vektor jeho součtem s násobkem jiného.

[4] Formulováním těchto tvrzení jako „pozorování“ a „důsledek“ jsme chytře nechali důkaz na čtenáři.

Věta 3.4. *Buďte* $\mathbb{A}, \mathbb{B} \in T^{m,n}$. *Je-li* $\mathbb{A} \sim \mathbb{B}$, *potom* $h(\mathbb{A}) = h(\mathbb{B})$.

Tvrzení 3.5. *Nechť* $\mathbb{A} \in T^{m,n}$ *je matice v horním stupňovitém tvaru s právě* k *nenulovými řádky. Pak* $h(\mathbb{A}) = k$.

Důkaz. Pro lineární obal souboru všech řádků $\mathbb{A}$ triviálně platí

$$\langle \mathbb{A}_{1:}, \ldots, \mathbb{A}_{m:} \rangle = \langle \mathbb{A}_{1:}, \ldots, \mathbb{A}_{k:} \rangle$$

(z LZ souboru lze odebrat nulový vektor a jeho lineární obal se nezmění), tedy $h(\mathbb{A}) = \dim\langle \mathbb{A}_{1:}, \ldots, \mathbb{A}_{k:} \rangle \leq k$.

Ukážeme-li, že soubor nenulových řádků matice $\mathbb{A}$ je navíc LN, bude platit rovnost $h(\mathbb{A}) = k$[5]. Uvažujme takovou lineární kombinaci nenulových řádků matice rovnou nulovému vektoru

$$\alpha_1 \mathbb{A}_{1:} + \cdots + \alpha_k \mathbb{A}_{k:} = \theta\,, \tag{3.1}$$

kde $\forall i \in \hat{k} : \alpha_i \in T$ (všechny uvažované vektory jsou zde řádkové, včetně nulového).

Nyní si stačí uvědomit, jak vypadá horní stupňovitý tvar. Označme jako v definici 1.25 pomocí $1 = j_1 < j_2 < \cdots < j_k$ indexy hlavních sloupců v horní stupňovité matici $\mathbb{A}$, postupnou úvahou dokážeme, že všechny koeficienty α_i v lineární kombinaci $\alpha_1 \mathbb{A}_{1:} + \cdots + \alpha_k \mathbb{A}_{k:} \in T^{1,n}$ musí být nulové[6].

- První složka lineární kombinace závisí pouze na $\alpha_1 \mathbb{A}_{1:}$ (v prvním sloupci jsou totiž kromě prvního řádku samé nuly). Jelikož v matici platí $\mathbb{A}_{11} \neq 0$ a lineární kombinace musí být rovna nulovému vektoru, musí platit $\alpha_1 = 0$ a první sčítanec lze z lineární kombinace vyškrtnout.

- Pro každý index $\ell \in \{2, \ldots, k\}$ postupně provedeme stejnou úvahu. Z horního stupňovitého tvaru plyne, že $j_\ell$tá složka lineární kombinace v (3.1) závisí pouze na sčítancích
$$\alpha_1 \mathbb{A}_{1:} + \cdots + \alpha_{\ell-1} \mathbb{A}_{(\ell-1):} + \alpha_\ell \mathbb{A}_{\ell:}$$
(skutečně, v $j_\ell$tém sloupci jsou pod ℓtým řádkem samé nuly), přitom všechny kromě posledního ℓtého sčítance jsou z předchozích kroků nulové. Současně v matici platí $\mathbb{A}_{\ell j_\ell} \neq 0$, tedy rovnost celé lineární kombinace nulovému vektoru implikuje $\alpha_\ell = 0$.

Tedy soubor k nenulových řádků matice $\mathbb{A}$ je LN a platí $h(\mathbb{A}) = k$. $\square$

Tvrzení bychom také mohli formulovat tak, že hodnost matice v horním stupňovitém tvaru je rovna počtu hlavních sloupců, jelikož se zřejmě jedná o stejné číslo, jako počet nenulových řádků.

---

[5]Proč? Protože tento soubor bude $k$prvkovou bází svého lineárního obalu.

[6]Zde nechť si kreativní čtenář představí (či nakreslí) schéma matice v horním stupňovitém tvaru a vyznačí si v něm hlavní sloupce.

Metody výpočtů (nejen) hodnosti

1. **Výpočet hodnosti matice:**
Máme-li spočítat $h(\mathbb{A})$, převedeme řádkovými úpravami GEM matici $\mathbb{A}$ na matici $\mathbb{B}$, která je v horním stupňovitém tvaru. Počet nenulových řádků matice $\mathbb{B}$ je roven $h(\mathbb{A})$.

2. **Výpočet dimenze lineárního obalu vektorů:**
Potřebujeme-li pro zadané vektory $x_1, \ldots x_m \in T^n$ spočítat $\dim\langle x_1, \ldots, x_m\rangle$, stačí vektory napsat do řádků matice a úpravami GEM převést tuto matici do horního stupňovitého tvaru. Počet nenulových řádků je pak hledaná dimenze.

3. **Ověření, zda vektor patří do lineárního obalu:**
Jsou dány $y, x_1, \ldots, x_m \in T^n$. Potřebujeme-li rozhodnout, zda
$$y \in \langle x_1, \ldots, x_m\rangle,$$
uvědomíme si, že toto platí právě tehdy, když
$$\langle x_1, \ldots, x_m\rangle = \langle x_1, \ldots, x_m, y\rangle.$$[7]
Jelikož se jedná o dva podprostory, které jsou v inkluzi, platí toto právě tehdy, když
$$\dim\langle x_1, \ldots, x_m\rangle = \dim\langle x_1, \ldots, x_m, y\rangle.$$
Tedy ověříme, zda hodnost matice, jejíž řádky jsou vektory $x_1, \ldots, x_m$, je stejná jako hodnost matice, ve které je navíc přidán řádek y.

4. **Ověření rovnosti lineárních obalů:**
Jsou dány $x_1, \ldots, x_r, y_1, \ldots, y_s \in T^n$. Potřebujeme-li ověřit, zda
$$\langle x_1, \ldots, x_r\rangle = \langle y_1, \ldots, y_s\rangle,$$
vzpomeneme si na pozorování 2.64, podle kterého jsou tyto dva lineární obaly rovny právě tehdy, když
$$\dim\langle x_1, \ldots, x_r\rangle = \dim\langle y_1, \ldots, y_s\rangle = \dim\langle x_1, \ldots, x_r, y_1, \ldots, y_s\rangle.$$
stačí ověřit rovnost hodností příslušných matic.

Poznámka 3.6. *K bodu 3 předchozího přehledu (ověření, zda vektor patří do lineárního obalu,* ***pouze*** *ve vektorovém prostoru typu T^n) jen poznamenejme, že postup přes hodnosti matic je jen jednou z možností. Jistě můžeme fakt*
$$y \in \langle x_1, \ldots, x_m\rangle \Leftrightarrow \exists \alpha_1 \ldots \alpha_m \in T : y = \sum_{i=1}^{m} \alpha_i x_i \tag{3.2}$$
ověřit i přímo z definice, přes řešitelnost soustavy lineárních rovnic v neznámých $\alpha_1 \ldots \alpha_m \in T$ (analogicky k algoritmu 2.68).

Tyto dva různé postupy důrazně rozlišujme!

[7] Jedna implikace plyne z pozorování 2.32. Laskavý čtenář nechť se sám zamyslí nad implikací opačnou.

1. *V postupu dle vztahu (3.2) řešíme SLR s maticí, která má všechny dané vektory zapsané* ***ve sloupcích*** *(navíc y určuje pravou stranu soustavy) a zajímá nás řešitelnost soustavy s neznámými $\alpha_1, \ldots, \alpha_n \in T$.*

2. *V postupu s využitím hodnosti pracujeme s maticí bez pravé strany, která má všechny dané vektory zapsané* ***v řádcích*** *a nic jako její řešení nás nezajímá! Pouze zkoumáme, kolik nenulových řádků zůstane po úpravě dvou matic na horní stupňovitý tvar – matice pouze s vektory x_i a matice s přidaným y.*

Rádi bychom zde čtenáře upozornili na další časté studentské nešvary stran definice hodnosti matice:

- Nikdy se nepokoušejte „definovat“ hodnost pomocí metody jejího výpočtu, tedy stylem *„hodnost je počet nenulových řádků potom, co udělám GEM“*. Korektnost takové definice závisí na tom, že ať už pomocí GEM převádíme matici do horního stupňovitého tvaru jakýmkoli konkrétním postupem, počet nulových řádků je přitom vždy stejný[8].

- Stejně tak důrazně varujeme před frázemi jako *„hodnost je maximální počet LN řádků matice“*, to je totiž také nesmysl! Lineární nezávislost je vlastnost souboru (nebo množiny) vektorů, nelze říci o jednom vektoru, že je nebo není LN.

- Ačkoli se to netýká přímo pojmu hodnost, prosíme všechny studenty, aby v žádné fázi klasifikačního procesu nepoužívali sousloví *„vyřeším matici“*[9]. Takový nešťastný výraz jen přivolává šťouravé dotazy zkoušejícího, cože to vlastně znamená to slovíčko *vyřešit* a jestlipak tomu dotyčný student rozumí. . .

Důkaz následující věty je poměrně složitý, proto ho neuvádíme a u zkoušky ho tedy nebudeme vyžadovat. Jde o jeden z hlavních výsledků o hodnosti matice – a to, že se nemění při transpozici[10].

Věta 3.7. *Nechť $\mathbb{A} \in T^{m,n}$. Potom*

$$h(\mathbb{A}) = h(\mathbb{A}^T).$$

Tato věta vlastně říká, že jsme mohli definovat hodnost jako dimenzi lineárního obalu souboru *sloupců* matice $\mathbb{A}$. Z toho také plyne následující tvrzení, které je triviálním důsledkem Steinitzovy věty (neboli tvrzení, že dimenze nemůže být větší, než počet generátorů).

Důsledek 3.8. *Nechť $\mathbb{A} \in T^{m,n}$. Potom $h(\mathbb{A}) \leq \min(m, n)$.*

[8] V očích zkoušejícího je navíc taková odpověď na otázku „co je to hodnost“ silně dehonestující. Protože student ví, jak něco spočítat, aniž by pořádně věděl, co to vlastně je!

[9] Nikde jej nepište a raději ani nahlas nevyslovujte!

[10] Což bychom také mohli (poněkud více slovy ale korektně) přeformulovat jako „dimenze lineárního obalu souboru řádků matice je rovna dimenzi lineárního obalu souboru jejích sloupců“.

3.3 Regulární matice a maticová inverze

Upozorňujeme čtenáře, že v některých následujících tvrzeních a definicích budeme předpokládat, že matice je **čtvercová** (tj. z $T^{n,n}$), a že pro nečtvercové matice by tato tvrzení či definice nedávala smysl.

Definice 3.9. ***Jednotkovou maticí*** *ntého řádu*[11] *rozumíme čtvercovou matici* $\mathbb{E} \in T^{n,n}$ *splňující*

$$\mathbb{E}_{ij} = \delta_{ij}\,, \quad i,j \in \hat{n}\,.$$

Diagonální maticí *ntého řádu nazveme libovolnou čtvercovou matici* $\mathbb{A} \in T^{n,n}$ *splňující*

$$i \neq j \Rightarrow \mathbb{A}_{ij} = 0\,.$$

Diagonálou *čtvercové matice* $\mathbb{A} \in T^{n,n}$ *nazveme vektor* $(\mathbb{A}_{11}, \mathbb{A}_{22}, \ldots, \mathbb{A}_{nn}) \in T^n$.

Doporučujeme čtenáři, aby si samostatně dokázal následující pozorování o násobení jednotkovou maticí. Stačí přitom použít přesný předpis pro maticové násobení a definici

$$\delta_{ij} = \begin{cases} 1, & \text{pro } i = j, \\ 0, & \text{jinak.} \end{cases}$$

Pozorování 3.10. *Pokud* $\mathbb{A}, \mathbb{E} \in T^{n,n}$, *pak* $\mathbb{A}\mathbb{E} = \mathbb{E}\mathbb{A} = \mathbb{A}$.

Tedy jednotková matice hraje v množině všech čtvercových matic $T^{n,n}$ roli *neutrálního prvku vůči operaci maticového násobení*[12]. A jak už to v životě[13] chodí, kdykoli někde narazíme na neutrální prvek k nějaké operaci, ihned jeho prostřednictvím definujeme prvky inverzní.

Definice 3.11. *Buď* $\mathbb{A} \in T^{n,n}$. *Existuje-li matice* $\mathbb{B} \in T^{n,n}$ *taková, že platí*

$$\mathbb{A}\mathbb{B} = \mathbb{B}\mathbb{A} = \mathbb{E},$$

nazýváme matici $\mathbb{A}$ ***regulární*** *a* $\mathbb{B}$ ***inverzní maticí*** *k matici* $\mathbb{A}$. *Značíme* $\mathbb{B} = \mathbb{A}^{-1}$. *Pokud* $\mathbb{A}$ *není regulární, nazýváme matici* $\mathbb{A}$ ***singulární***.

Na definici rovnou navážeme jednoduchými tvrzeními o jednoznačnosti inverze a o inverzi součinu regulárních matic.

Věta 3.12. *Je-li* $\mathbb{A} \in T^{n,n}$ *regulární, potom je inverzní matice k* $\mathbb{A}$ *určena jednoznačně.*

Důkaz. Předpokládejme, že existují dvě matice $\mathbb{B}_1, \mathbb{B}_2 \in T^{n,n}$ takové, že

$$\mathbb{A}\mathbb{B}_1 = \mathbb{B}_1\mathbb{A} = \mathbb{E} \quad \text{a současně} \quad \mathbb{A}\mathbb{B}_2 = \mathbb{B}_2\mathbb{A} = \mathbb{E}.$$

[11] Nebo prostě typu $n \times n$.

[12] Fajnšmekři znalí obecné algebry mohou množinu všech čtvercových matic $T^{n,n}$ s operací násobení klidně nazvat *monoidem* – ví-li, o co jde…

[13] Tedy v matematických předmětech.

Ukážeme, že z toho již nutně vyplývá rovnost $\mathbb{B}_1 = \mathbb{B}_2$. Použitím asociativního zákona pro maticové násobení dostáváme

$$\mathbb{B}_1 = \mathbb{B}_1\mathbb{E} = \mathbb{B}_1 \underbrace{(\mathbb{A}\mathbb{B}_2)}_{=\mathbb{E}} = \underbrace{(\mathbb{B}_1\mathbb{A})}_{=\mathbb{E}} \mathbb{B}_2 = \mathbb{E}\mathbb{B}_2 = \mathbb{B}_2$$

a důkaz je hotov. □

Věta 3.13. *Nechť $\mathbb{A}, \mathbb{B} \in T^{n,n}$ jsou regulární, potom $\mathbb{A}\mathbb{B}$ je také regulární a platí*

$$(\mathbb{A}\mathbb{B})^{-1} = \mathbb{B}^{-1}\mathbb{A}^{-1}.$$

Důkaz. Větu dokážeme přímým dosazením. Dokážeme, že $\mathbb{B}^{-1}\mathbb{A}^{-1}$ je opravdu inverzní k zadanému součinu $\mathbb{A}\mathbb{B}$, přitom využijeme jen definice inverzní matice a asociativního zákona. Protože

$$(\mathbb{A}\mathbb{B})(\mathbb{B}^{-1}\mathbb{A}^{-1}) = \mathbb{A}(\mathbb{B}\mathbb{B}^{-1})\mathbb{A}^{-1} = \mathbb{A}\mathbb{A}^{-1} = \mathbb{E}$$

a analogicky

$$(\mathbb{B}^{-1}\mathbb{A}^{-1})(\mathbb{A}\mathbb{B}) = \mathbb{B}^{-1}(\mathbb{A}^{-1}\mathbb{A})\mathbb{B} = \mathbb{B}^{-1}\mathbb{B} = \mathbb{E},$$

je podle definice matice $\mathbb{A}\mathbb{B}$ regulární a platí $(\mathbb{A}\mathbb{B})^{-1} = \mathbb{B}^{-1}\mathbb{A}^{-1}$. □

Aby $\mathbb{B}$ byla inverzní maticí k $\mathbb{A}$, musí podle definice platit dvě rovnosti:

$$\mathbb{A}\mathbb{B} = \mathbb{E} \quad \text{a} \quad \mathbb{B}\mathbb{A} = \mathbb{E}.$$

Lze ovšem ukázat, že k regularitě matice $\mathbb{A}$ vlastně stačí, aby platila pouze jedna z rovností výše. Druhá je potom automaticky také splněna. K důkazu tohoto tvrzení ovšem potřebujeme hlubší znalosti o *lineárních zobrazeních*, ty doposud nemáme ani definovány, proto důkaz přeskočíme. Čtenářům zde nicméně slavnostně slibujeme, že tento hřích napravíme v jedné z následujících kapitol, s názvem Lineární zobrazení!

Věta 3.14. *Buď $\mathbb{A} \in T^{n,n}$. Existuje-li $\mathbb{B} \in T^{n,n}$ taková, že platí $\mathbb{A}\mathbb{B} = \mathbb{E}$ nebo $\mathbb{B}\mathbb{A} = \mathbb{E}$, potom je $\mathbb{A}$ regulární a $\mathbb{B} = \mathbb{A}^{-1}$.*

Důkaz. Provedeme v kapitole Lineární zobrazení. □

Maticová interpretace GEM

Upozorňujeme, že v této části pro jednoduchost značíme upravovanou matici pouze jako $\mathbb{A}$ i přesto, že většinou při GEM pracujeme s rozšířenými maticemi soustav ve tvaru $(\mathbb{A}|\mathbb{b})$. Nejde o žádnou újmu na korektnosti, dobře si totiž uvědomujeme, že oddělovač v rozšířené matici soustavy kromě vizuálního odlišení pravé strany žádnou jinou roli nehraje a rozšířená matice je prostě klasická matice.

Řádkové úpravy Gaussovy eliminační metody v matici $\mathbb{A} \in T^{m,n}$ lze realizovat tak, že $\mathbb{A}$ vynásobíme **zleva** vhodnou regulární maticí $\mathbb{P} \in T^{m,m}$. Všechna tvrzení uvedená níže si jistě každý student sám **ověří**[14]:

[14]S využitím definice maticového násobení a bez jakýchkoli obav z dosazování obecných matic!

1. Prohození $i$tého a $j$tého řádku: Matici $\mathbb{P}(i,j) \in T^{m,m}$ definujeme:

$$[\mathbb{P}(i,j)]_{k\ell} := \begin{cases} 1, & \text{pokud } (\, k = \ell \notin \{i,j\}\,) \vee (k = i \wedge \ell = j) \vee (k = j \wedge \ell = i) \\ 0, & \text{jinak,} \end{cases}$$

tedy $\mathbb{P}(i,j)$ je matice vzniklá z jednotkové matice $\mathbb{E} \in T^{m,m}$ prohozením $i$tého a $j$tého řádku.

- Matice $\mathbb{P}(i,j)\mathbb{A}$ je matice $\mathbb{A}$ s prohozeným $i$tým a $j$tým řádkem. (Ověřte!)
- Matice $\mathbb{P}(i,j)$ je regulární a platí

$$\Big(\mathbb{P}(i,j)\Big)^{-1} = \mathbb{P}(i,j).$$

2. Vynásobení $i$tého řádku číslem $\alpha \neq 0$: Matici $\mathbb{P}_i(\alpha) \in T^{m,m}$ definujeme:

$$[\mathbb{P}_i(\alpha)]_{k\ell} := \begin{cases} \alpha, & \text{pokud } k = \ell = i \\ 1, & \text{pokud } k = \ell \neq i \\ 0, & \text{jinak,} \end{cases}$$

tedy $\mathbb{P}_i(\alpha)$ je (diagonální) matice vzniklá z jednotkové matice $\mathbb{E} \in T^{m,m}$ nahrazením čísla 1 na $i$té pozici na diagonále číslem α.

- Matice $\mathbb{P}_i(\alpha)\mathbb{A}$ je matice $\mathbb{A}$ s $i$tým řádkem vynásobeným číslem α.
- Matice $\mathbb{P}_i(\alpha)$ je regulární (pro $\alpha \neq 0$) a platí

$$\Big(\mathbb{P}_i(\alpha)\Big)^{-1} = \mathbb{P}_i(\alpha^{-1}).$$

3. Přičtení αnásobku $i$tého řádku k $j$tému řádku: Matici $\mathbb{Q}_{i,j}(\alpha) \in T^{m,m}$ pro $i \neq j$ definujeme takto:

$$[\mathbb{Q}_{i,j}(\alpha)]_{k\ell} := \begin{cases} \alpha, & \text{pokud } k = j \wedge \ell = i \\ 1, & \text{pokud } k = \ell \\ 0, & \text{jinak,} \end{cases}$$

tedy $\mathbb{Q}_{i,j}(\alpha)$ je matice vzniklá z jednotkové matice $\mathbb{E} \in T^{m,m}$ přidáním čísla $\alpha \in T$ na (j,i)-tou pozici.

- Matice $\mathbb{Q}_{i,j}(\alpha)\mathbb{A}$ je matice $\mathbb{A}$ po přičtení αnásobku $i$tého řádku k j-tému. Tedy

$$\Big(\mathbb{Q}_{i,j}(\alpha)\mathbb{A}\Big)_{j:} = \mathbb{A}_{j:} + \alpha\mathbb{A}_{i:}\,.$$

- Matice $\mathbb{Q}_{i,j}(\alpha)$ je regulární a platí

$$\Big(\mathbb{Q}_{i,j}(\alpha)\Big)^{-1} = \mathbb{Q}_{i,j}(-\alpha).$$

Důsledek 3.15. *Nechť* $\mathbb{A}, \mathbb{B} \in T^{m,n}$ *a* $\mathbb{A} \sim \mathbb{B}$*. Potom* $\exists \mathbb{P} \in T^{m,m}$ *regulární taková, že* $\mathbb{B} = \mathbb{P}\mathbb{A}$*.*

Důkaz. Matice $\mathbb{B}$ vznikla z $\mathbb{A}$ konečnou posloupností elementárních kroků (G1)-(G3) GEM, které lze realizovat vynásobením matice $\mathbb{A}$ zleva popořadě regulárními maticemi $\mathbb{P}_1, \dots, \mathbb{P}_n \in T^{m,m}$ (každá z nich je nějakého z výše uvedených tří typů). Tedy $\mathbb{B} = \mathbb{P}_n \dots \mathbb{P}_1 \mathbb{A}$. Protože součin regulárních matic je regulární matice, položíme $\mathbb{P} := \mathbb{P}_n \dots \mathbb{P}_1$ a dostaneme tvrzení věty. $\square$

Poznámka 3.16. *Analogicky bychom místo řádkových úprav mohli používat 3 typy odpovídajících* ***elementárních sloupcových úprav****, i pro ně bychom opět sestavili 3 typy regulárních matic realizující jednotlivé kroky. Matici* $\mathbb{A}$ *bychom tentokrát násobili regulární maticí zprava. Nalezení takových matic realizující sloupcové analogie ke krokům GEM ponecháváme zvídavému čtenáři jako jednoduché cvičení.*

Upozorněme ale, že samozřejmě ***nelze*** *jen tak používat sloupcové úpravy namísto řádkových. Při námi zavedeném maticovém zápisu soustav, kde řádky korespondují s rovnicemi a sloupce s neznámými, by sloupcové úpravy neměly valného smyslu!*[15]

O regulárních maticích

Jedna z klíčových vět této kapitoly nám řekne, s čím vším je *ekvivalentní* regularita čtvercové matice.

Věta 3.17. *Buď* $\mathbb{A} \in T^{n,n}$*. Následující tvrzení jsou ekvivalentní.*

(i) $\mathbb{A}$ *je regulární.*

(ii) Soubor řádků matice $\mathbb{A}$ *je LN.*

(iii) $h(\mathbb{A}) = n$*.*

(iv) $\mathbb{A} \sim \mathbb{E}$*.*

Důkaz. Dokážeme řetězec implikací $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (i)$, každé tvrzení pak bude ekvivalentní s každým.

(i) $\Rightarrow$ (ii): Předpokládáme regularitu $\mathbb{A}$, tedy dle definice existuje inverzní matice $\mathbb{A}^{-1}$. Podívejme se na libovolnou lineární kombinaci řádků $\mathbb{A}$ a předpokládejme, že se rovná nulovému vektoru (rovněž řádkovému),

$$\sum_{i=1}^{n} \beta_i \mathbb{A}_{i:} = \theta. \tag{3.3}$$

Ukážeme, že z toho vyplývá, $\beta_1 = \cdots = \beta_n = 0$. Označme řádkový vektor koeficientů jako $\mathbb{b} = (\beta_1, \dots, \beta_n)$, odvodíme přepis rovnice (3.3) do jiného

[15]Nic nám samozřejmě nebrání elementární sloupcové úpravy definovat. To že se příliš nehodí k řešení SLR neznamená, že se nemohou hodit k ničemu jinému.

tvaru. Jelikož rovnost dvou vektorů implikuje rovnost jejich příslušných složek, přechází rovnice (3.3) v soustavu rovnic

$$\forall j \in \hat{n} : \left(\sum_{i=1}^{n} \beta_i \mathbb{A}_{i:} \right)_j = 0\,,$$

neboli

$$\forall j \in \hat{n} : \sum_{i=1}^{n} \beta_i \mathbb{A}_{ij} = 0\,,$$

což lze pomocí maticového násobení přepsat jednoduše jako

$$\mathbb{b} \cdot \mathbb{A} = \theta.$$

Protože předpokládáme, že $\mathbb{A}$ je regulární, můžeme obě strany poslední rovnosti vynásobit maticí $\mathbb{A}^{-1}$ zprava. Dostaneme $\mathbb{b} = \theta$, a tedy $\beta_1 = \cdots = \beta_n = 0$. Proto je soubor řádků $(\mathbb{A}_{1:}, \ldots, \mathbb{A}_{n:})$ lineárně nezávislý.

(ii) ⇒ (iii): Vyplývá ihned z definice hodnosti matice.

(iii) ⇒ (iv): Předpokládáme, že dimenze lineárního obalu souboru řádků čtvercové matice $\mathbb{A}$ je maximální, tedy n, a ta se aplikací elementárních úprav GEM nemění. Převedeme-li $\mathbb{A}$ na matici v horním stupňovitém tvaru (označme ji $\mathbb{X}$), musí být tato výsledná matice už rovnou horní trojúhelníková a nemá žádný nulový řádek (jinak by platilo $h(\mathbb{A}) < n$). Na diagonále $\mathbb{X}$ musí být navíc nutně všechny prvky nenulové.

Snadno si pak lze rozmyslet, že matici $\mathbb{X}$ lze řádkovými úpravami převést na jednotkovou matici $\mathbb{E}$. Vhodným přičítáním násobků posledního řádku ke všem ostatním lze vyrobit nuly v celém posledním sloupci (kromě diagonálního prvku), poté lze přičítáním násobků předposledního řádku ke všem nad ním vyrobit nuly v předposledním sloupci, a tak dále. Výslednou diagonální matici pak převedeme na $\mathbb{E}$ jen vydělením každého řádku příslušným prvkem na diagonále. Celkem tedy máme

$$\mathbb{A} \sim \mathbb{X} \sim \mathbb{E}.$$

(iv) ⇒ (i): Protože $\mathbb{A} \sim \mathbb{E}$, víme, že existuje regulární matice $\mathbb{P} \in T^{n,n}$ taková, že

$$\mathbb{P}\mathbb{A} = \mathbb{E}\,.$$

K $\mathbb{P}$ navíc existuje inverze, kterou můžeme celou rovnici (zleva) vynásobit, tedy

$$\mathbb{A} = \mathbb{P}^{-1}\mathbb{P}\mathbb{A} = \mathbb{P}^{-1}\mathbb{E} = \mathbb{P}^{-1}\,,$$

matice $\mathbb{A}$ se rovná regulární matici $\mathbb{P}^{-1}$ a je sama regulární. □

Poznámka 3.18. *Protože víme, že $h(\mathbb{A}) = h(\mathbb{A}^T)$, platí také ekvivalence:*

$$\mathbb{A} \textit{ je regulární } \Leftrightarrow \textit{ soubor sloupců matice } \mathbb{A} \textit{ je LN.}$$

Z věty 3.17 pro nás vyplývá extrémně užitečný nástroj k počítání inverzních matic. Jak už víme, posloupnost jednotlivých kroků GEM lze realizovat vynásobením matice $\mathbb{A}$ zleva nějakou regulární maticí $\mathbb{P}$. Je-li $\mathbb{A}$ regulární, můžeme dostat

$$\mathbb{PA} = \mathbb{E}$$

a z definice inverzní matice pak plyne $\mathbb{A}^{-1} = \mathbb{P}$. Následující algoritmus pracuje s myšlenkou, že provádíme-li tytéž úpravy současně na matici $\mathbb{A}$ a na jednotkové matici $\mathbb{E}$ stejného rozměru, pak z jednotkové matice vznikne $\mathbb{E} \sim \mathbb{PE} = \mathbb{P} = \mathbb{A}^{-1}$, tedy hledaná inverze.

Algoritmus 3.19 (Ověření regularity a nalezení inverzní matice)**.** *Nechť* $\mathbb{A} \in T^{n,n}$*. Ověřte, zda je matice regulární a pokud je, nalezněte k ní matici inverzní* $\mathbb{A}^{-1}$*.*

1. *Hledáme matici* $\mathbb{A}^{-1}$ *s vlastností* $\mathbb{A}^{-1}\mathbb{A} = \mathbb{A}\mathbb{A}^{-1} = \mathbb{E}$*.*

2. *Doplněním zadané matice o jednotkovou matici stejného rozměru sestavme dvoublokovou rozšířenou matici* $(\mathbb{A} \mid \mathbb{E}) \in T^{n,2n}$*.*

3. *Na celou* $(\mathbb{A} \mid \mathbb{E})$ *používáme řádkové úpravy GEM, pro libovolnou posloupnost řádkových úprav realizovaných regulární maticí* $\mathbb{P}$ *pak platí*

$$(\mathbb{A} \mid \mathbb{E}) \sim (\mathbb{PA} \mid \mathbb{PE}) = (\mathbb{PA} \mid \mathbb{P}) .$$

   Díky větě 3.17 platí, že levý blok $\mathbb{A}$ *je možné převést na jednotkovou matici právě tehdy, když je* $\mathbb{A}$ *regulární. Vznikne-li při úpravách* $\mathbb{A}$ *na horní stupňovitý tvar nulový řádek, pak* $\mathbb{A}$ *je singulární a inverze neexistuje.*

4. *Je-li* $\mathbb{A}$ *regulární, pak pro úpravy* $\mathbb{P}$ *vedoucí k převedení levého bloku matice* $(\mathbb{A} \mid \mathbb{E})$ *na jednotkovou matici platí* $\mathbb{P} = \mathbb{A}^{-1}$*, tedy*

$$(\mathbb{A} \mid \mathbb{E}) \sim (\mathbb{E} \mid \mathbb{A}^{-1})$$

   a pravý blok výsledné matice obsahuje hledanou $\mathbb{A}^{-1}$*.*

Tuto část uzavřeme dvěma poznatky o násobení regulární maticí. Prozatím víme, že každá konečná posloupnost kroků GEM se dá realizovat násobením zleva nějakou regulární maticí. Ukážeme si, že to platí i obráceně, tedy že každá regulární matice reprezentuje nějakou konečnou posloupnost kroků GEM.

Věta 3.20. *Nechť* $\mathbb{A}, \mathbb{B} \in T^{m,n}$*. Existuje-li* $\mathbb{P} \in T^{m,m}$ *regulární taková, že* $\mathbb{B} = \mathbb{PA}$*, potom* $\mathbb{A} \sim \mathbb{B}$*.*

Důkaz. Matice $\mathbb{P}$ je regulární, proto $\mathbb{P} \sim \mathbb{E}$. Nechť tuto eliminaci realizuje regulární matice $\mathbb{Q}$, tedy $\mathbb{QP} = \mathbb{E}$. Aplikujeme-li stejné kroky GEM jako při eliminaci $\mathbb{P} \sim \mathbb{E}$ na matici $\mathbb{B}$ dostaneme matici $\mathbb{A}$, protože

$$\mathbb{QB} = \mathbb{QPA} = \mathbb{EA} = \mathbb{A}.$$

Tedy $\mathbb{B} \sim \mathbb{A}$ a z vratnosti všech elementárních kroků GEM platí i $\mathbb{A} \sim \mathbb{B}$. □

Důsledek 3.21. *Násobením regulární maticí se hodnost nezmění. Tedy je-li* $\mathbb{A} \in T^{m,n}$ *libovolná a* $\mathbb{P} \in T^{m,m}$ *regulární, platí*

$$h(\mathbb{A}) = h(\mathbb{PA}).$$

Důkaz. Víme, že $\mathbb{A} \sim \mathbb{PA}$. Stačí využít toho, že GEM nemění hodnost matice. □

3.4 Frobeniova věta a kompletní řešení SLR

Na začátek poznamenejme, že o množinách řešení soustav lineárních rovnic už mnohé víme. Čtenář si jistě rád pro osvěžení vzpomínek nalistuje první kapitolu, dříve zavedené značení nebudeme nijak dramaticky měnit[16]. Pro jistotu zopakujme:

- řešíme soustavy $\mathbb{A}\mathbb{x} = \mathbb{b}$ (zapisujeme $(\mathbb{A} \mid \mathbb{b})$), kde
- $\mathbb{A} = (\alpha_{ij})_{i\in\hat{m}, j\in\hat{n}} \in T^{m,n}$ je matice soustavy,
- $\mathbb{b} = (\beta_1 \ \cdots \ \beta_m)^T \in T^{m,1}$ je (sloupcový) vektor pravých stran,
- $\mathbb{x} = (x_1 \ \cdots \ x_n)^T \in T^{n,1}$ je (sloupcový) vektor neznámých,
- S je množina všech řešení soustavy $\mathbb{A}\mathbb{x} = \mathbb{b}$,
- S_0 je množina všech řešení přidružené homogenní soustavy $\mathbb{A}\mathbb{x} = \theta$ (kde $\theta = (0 \ \cdots \ 0)^T$).

Co se týká homogenních soustav, můžeme rovnou formulovat základní vlastnost množiny S_0, a to s využitím nově zavedených pojmů. Uvědomíme-li si triviální pravdu, že řešení homogenní SLR vždy existuje (alespoň nulový vektor $\theta \in T^{n,1}$), pak z částí již dokázané věty 1.19 rovnou plyne jednoduché pozorování.

Pozorování 3.22. *Množina S_0 všech řešení homogenní soustavy $\mathbb{A}\mathbb{x} = \theta$ je podprostor ve VP $T^{n,1}$.*

Předtím, než přejdeme k hlavnímu výsledku, dokážeme si v následujícím lemmatu[17] několik jednoduchých tvrzení).

Lemma 3.23. *Nechť $\mathbb{A} \in T^{m,n}$.*

(i) Nechť $\mathbb{x}_1, \dots, \mathbb{x}_k \in T^{n,1}$ a $\alpha_1, \dots, \alpha_k \in T$. Pak

$$\mathbb{A}\Big(\sum_{i=1}^{k} \alpha_i \mathbb{x}_i\Big) = \sum_{i=1}^{k} \alpha_i (\mathbb{A}\mathbb{x}_i)\,.$$

(ii) Pro libovolné $\mathbb{y} \in \langle \mathbb{A}_{:1}, \dots, \mathbb{A}_{:n} \rangle \subset\subset T^{m,1}$ existuje $\mathbb{x} \in T^{n,1}$ takové, že $\mathbb{y} = \mathbb{A}\mathbb{x}$.

(iii) Nechť $\mathbb{x}_1, \dots, \mathbb{x}_k \in T^{n,1}$, $\mathbb{y}_1, \dots, \mathbb{y}_k \in T^{m,1}$ splňují $\mathbb{A}\mathbb{x}_i = \mathbb{y}_i$ pro každé $i \in \hat{k}$. Pak platí

$$(\mathbb{y}_1, \dots, \mathbb{y}_k) \text{ je LN} \quad \Rightarrow \quad (\mathbb{x}_1, \dots, \mathbb{x}_k) \text{ je LN}.$$

Důkaz. (i) Zřejmě vyplývá ze základních vlastností násobení matic.

[16] Přeznačení koeficientů v soustavě rovnic $a_{ij} \to \alpha_{ij}$ a $b_i \to \beta_i$ by nikomu zkazit den nemělo.

[17] Lemma je jen vysoce sofistikované označení pro pomocné tvrzení (které si z nějakého důvodu nezaslouží označení věta) užitečné při důkazu jiného sofistikovanějšího tvrzení (které si označení věta už zaslouží).

(ii) Označíme-li (sloupcové) vektory standardní báze v $T^{n,1}$ jako $\mathbb{e}_1, \dots, \mathbb{e}_n$[18], jednoduše nahlédneme, že každý sloupec matice $\mathbb{A}$ lze získat součinem

$$\mathbb{A}_{:j} = \mathbb{A}\mathbb{e}_j \,.$$

Je-li nějaký vektor $\mathbb{y} \in T^{m,1}$ lineární kombinací sloupců matice $\mathbb{A}$, existují $\alpha_1, \dots, \alpha_n \in T$ takové, že

$$\mathbb{y} = \sum_{i=1}^{n} \alpha_i(\mathbb{A}\mathbb{e}_i) = \mathbb{A}\Bigl(\sum_{i=1}^{n} \alpha_i \mathbb{e}_i\Bigr) \,,$$

přičemž jsme využili předchozí bod (i). Hledaným vektorem $\mathbb{x}$ je zřejmě

$$\mathbb{x} = \sum_{i=1}^{n} \alpha_i \mathbb{e}_i = (\alpha_1 \ \cdots \ \alpha_n)^T \,.$$

(iii) Předpokládejme, že soubor $(\mathbb{y}_1, \dots, \mathbb{y}_k) = (\mathbb{A}\mathbb{x}_1, \dots, \mathbb{A}\mathbb{x}_k)$ je lineárně nezávislý. Nechť $\beta_1, \dots, \beta_k \in T$ a platí $\sum_{i=1}^{k} \beta_i \mathbb{x}_i = \theta$. Vynásobením obou stran rovnice maticí $\mathbb{A}$ dostáváme s použitím bodu (i)

$$\theta \overset{[19]}{=} \mathbb{A}\theta = \mathbb{A}\Bigl(\sum_{i=1}^{k} \beta_i \mathbb{x}_i\Bigr) = \sum_{i=1}^{k} \beta_i \underbrace{(\mathbb{A}\mathbb{x}_i)}_{=\mathbb{y}_i} \,.$$

Jelikož pouze triviální lineární kombinace LN souboru se může rovnat nulovému vektoru, platí $\beta_1 = \cdots = \beta_k = 0$.

□

Následující hlavní výsledek budeme v celém kurzu titulovat „Frobeniova věta“[20], ačkoli celosvětově to není s jejím autorstvím tak jednoduché. Pokusí-li se student vyhledat pojem „Frobenius theorem“, narazí pravděpodobně na úplně jiný výsledek, ať už o vlastních číslech kladných matic, či z oblasti zvané diferenciální geometrie[21]. Jakési mezinárodní označení následujícího výsledku je „Rouché–Capelli theorem“, ale v závislosti na zemi se jako označení autorů volí různé podmnožiny z pětice Capelli–Fontené–Frobenius–Kronecker–Rouché[22]. Současně lze narazit na různé varianty této věty, někde se jako její součást uvádí pouze bod (i), někde oba.

Věta 3.24 (Frobeniova)**.** *Nechť $\mathbb{A} \in T^{m,n}$.*

(i) Soustava m lineárních rovnic pro n neznámých $\mathbb{A}\mathbb{x} = \mathbb{b}$ je řešitelná, tj. $S \neq \emptyset$, právě tehdy, když

$$h(\mathbb{A}) = h(\mathbb{A} \mid \mathbb{b}).$$

---

[18]Tedy $\mathbb{e}_1 = (1\ 0\ \dots\ 0)^T, \mathbb{e}_2 = (0\ 1\ \dots\ 0)^T, \dots, \mathbb{e}_n = (0\ \dots\ 0\ 1)^T$.

[19]Jen pro jistotu připomeňme, že není théta jako théta! V rovnosti $\mathbb{A}\theta = \theta$ je jedna nulovým vektorem $T^{n,1}$ a jedna nulovým vektorem $T^{m,1}$.

[20]Řekněme, že je to důsledek takové naší lokální tradice.

[21]Pan Frobenius toho dokázal poměrně hodně.

[22]Důvody mohou být společná historie a kulturní vliv (Frobenius u nás, případně Kronecker–Capelli shodně v Rusku, Polsku a Maďarsku), případně „fandění domácímu týmu“ (Rouché–Fontené ve Francii)

(ii) Je-li $h(\mathbb{A}) = h$, pak množina řešení soustavy $\mathbb{A}\mathbb{x} = \theta$ je podprostor dimenze $n - h$, tedy existuje LN soubor vektorů $(\mathbb{z}_1, \ldots, \mathbb{z}_{n-h})$ v $T^{n,1}$ takový, že

$$S_0 = \begin{cases} \{\theta\}, & \text{pokud } n = h, \\ \langle \mathbb{z}_1, \ldots, \mathbb{z}_{n-h} \rangle, & \text{pokud } h < n. \end{cases}$$

Je-li navíc $h(\mathbb{A} \mid \mathbb{b}) = h$, pak

$$S = \tilde{\mathbb{x}} + S_0,$$

*kde $\tilde{\mathbb{x}}$ je tzv. **partikulární řešení:** $\mathbb{A}\tilde{\mathbb{x}} = \mathbb{b}$.*

Důkaz. Na tomto místě poznamenejme, že v kurzu budeme vyžadovat pouze důkaz bodu (i). Důkaz bodu (ii) nechť velectěný čtenář považuje za zajímavost a dobrovolný bonus.

(i) **($\Rightarrow$) :** Nechť $\mathbb{y} = (y_1, \ldots, y_n)^T$ je řešením soustavy $\mathbb{A}\mathbb{x} = \mathbb{b}$, tedy platí

$$\forall i \in \hat{m} : \sum_{j=1}^{n} \alpha_{ij} y_j = \beta_i \,.$$

Skutečnost $\mathbb{A}\mathbb{y} = \mathbb{b}$ lze také přepsat jinak, a to jako

$$\sum_{j=1}^{n} y_j \mathbb{A}_{:j} = \mathbb{b}\,, \tag{3.4}$$

tedy že složky řešení $y_1, \ldots, y_n$ jsou vlastně koeficienty v takové lineární kombinaci **sloupců** matice $\mathbb{A}$, která je rovna vektoru pravé strany $\mathbb{b}$. Skutečně, pokud si rovnici (3.4) rozepíšeme podrobněji,

$$y_1 \begin{pmatrix} \alpha_{11} \\ \alpha_{21} \\ \vdots \\ \alpha_{m1} \end{pmatrix} + y_2 \begin{pmatrix} \alpha_{12} \\ \alpha_{22} \\ \vdots \\ \alpha_{m2} \end{pmatrix} + \cdots + y_n \begin{pmatrix} \alpha_{1n} \\ \alpha_{2n} \\ \vdots \\ \alpha_{mn} \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_m \end{pmatrix},$$

snáze uvidíme, že je rovnici $\mathbb{A}\mathbb{y} = \mathbb{b}$ opravdu ekvivalentní [23].

Dostáváme tedy fakt

$$\mathbb{b} \in \langle \mathbb{A}_{:1}, \ldots, \mathbb{A}_{:n} \rangle\,,$$

z čehož nutně plyne

$$\langle \mathbb{A}_{:1}, \ldots, \mathbb{A}_{:n} \rangle = \langle \mathbb{A}_{:1}, \ldots, \mathbb{A}_{:n}, \mathbb{b} \rangle$$

a rovnost musí platit i pro dimenze těchto lineárních obalů. Protože z dříve dokázaného tvrzení platí, že hodnost matice je rovna jak dimenzi lineárního obalu souboru svých řádků, tak i dimenzi lineárního obalu souboru svých sloupců, platí $h(\mathbb{A}) = h(\mathbb{A} \mid \mathbb{b})$.

[23] Toto nechť si každý čtenář nechá důkladně projít hlavou.

($\Leftarrow$) : Nechť $h(\mathbb{A}) = h(\mathbb{A} \mid \mathbb{b})$. Protože platí

$$\langle \mathbb{A}_{:1}, \dots, \mathbb{A}_{:n} \rangle \subset\subset \langle \mathbb{A}_{:1}, \dots, \mathbb{A}_{:n}, \mathbb{b} \rangle$$

a současně mají tyto podprostory v $T^{m,1}$ stejnou konečnou dimenzi, musí platit dle důsledku 2.58, že

$$\langle \mathbb{A}_{:1}, \dots, \mathbb{A}_{:n} \rangle = \langle \mathbb{A}_{:1}, \dots, \mathbb{A}_{:n}, \mathbb{b} \rangle.$$

Speciálně tedy

$$\mathbb{b} \in \langle \mathbb{A}_{:1}, \dots, \mathbb{A}_{:n} \rangle,$$

a proto existují $y_1, \dots, y_n \in T$ tak, že

$$\mathbb{b} = \sum_{j=1}^{n} y_j \mathbb{A}_{:j},$$

neboli $\mathbb{A}\mathbb{y} = \mathbb{b}$ (opět, podobně jako výše, dle sloupcové interpretace soustavy!), kde $\mathbb{y} = (y_1, \dots, y_n)^T$. Soustava $\mathbb{A}\mathbb{x} = \mathbb{b}$ tedy má řešení $\mathbb{y} \in S$.

(ii) Fakt, že pro každou řešitelnou soustavu platí

$$S = \tilde{\mathbb{x}} + S_0,$$

kde $\tilde{\mathbb{x}}$ je nějaké řešení, už máme dokázaný z dřívějška (věta 1.22), pouze zavádíme nový pojem, **partikulární řešení**. Zbývá nám tedy dokázat, že všechna řešení homogenní soustavy tvoří podprostor dimenze právě $n - h(\mathbb{A})$[24], dokážeme vztah

$$h(\mathbb{A}) + \dim S_0 = n\,.$$

Začneme triviálním případem, kdy $h(\mathbb{A}) = 0$. Snadno nahlédneme, že matice soustavy pak musí být nutně nulová, $\mathbb{A} = \Theta$. Řešením soustavy s takovou maticí je libovolný vektor $\mathbb{x} \in T^{n,1}$, tedy $S_0 = T^{n,1}$ a $\dim S_0 = n$.

Ve zbytku důkazu předpokládejme, že $h(\mathbb{A}) = h \in \mathbb{N}$.

Připomeňme, že máme k dispozici 1. větu o dimenzi (věta 2.63) a že platí $\dim T^{n,1} = n$. Našim cílem bude nalezení takového podprostoru $P \subset\subset T^{n,1}$, pro který bude platit $\dim P = h$ a současně $P \oplus S_0 = T^{n,1}$[25]. Z toho rovnou vyplyne $\dim S_0 = n - h$.

Uvažujme soubor sloupců matice $\mathbb{A}$, platí

$$h = \dim \underbrace{\langle \mathbb{A}_{:1}, \dots, \mathbb{A}_{:n} \rangle}_{\subset\subset T^{m,1}}\,.$$

[24] Že jde o podprostor už samozřejmě víme, jde nám jen o jeho dimenzi.
[25] Značení pro direktní součet podprostorů jistě nikoho nepřekvapí.

Označme jako $(\mathbb{y}_1, \dots \mathbb{y}_h)$ nějakou bázi lineárního obalu $\langle \mathbb{A}_{:1}, \dots, \mathbb{A}_{:n} \rangle$. Jistě pro každé $i \in \hat{h}$ platí, že $\mathbb{y}_i \in \langle \mathbb{A}_{:1}, \dots, \mathbb{A}_{:n} \rangle$. Pak z lemmatu 3.23 plyne existence LN souboru $(\mathbb{x}_1, \dots, \mathbb{x}_h)$ v prostoru $T^{n,1}$, pro který platí

$$\forall i \in \hat{h} : \ \mathbb{y}_i = \mathbb{A}\mathbb{x}_i \, .$$

Nalezli jsme tedy podprostor $P = \langle \mathbb{x}_1, \dots, \mathbb{x}_h \rangle \subset\subset T^{n,1}$ o dimenzi $h \in \mathbb{N}$. Dokážeme $P \oplus S_0 = T^{n,1}$, tedy že jeho součet s množinou řešení homogenní soustavy dá celé $T^{n,1}$ a je navíc direktní.

- Zřejmě platí $P + S_0 \subseteq T^{n,1}$, dokážeme opačnou inkluzi. Nechť $\mathbb{x} \in T^{n,1}$, ověříme, že existuje jeho rozklad
$$\mathbb{x} = \underbrace{\mathbb{p}}_{\in P} + \underbrace{\mathbb{q}}_{\in S_0} \, . \tag{3.5}$$
Jelikož $\mathbb{p} \in P$, platí $\mathbb{p} = \sum_{i=1}^{h} \alpha_i \mathbb{x}_i$ pro nějaké $\alpha_1, \dots, \alpha_h \in T$. Vyjádříme-li z (3.5) vektor $\mathbb{q} \in S_0$ a vynásobíme-li obě strany rovnice maticí $\mathbb{A}$, dostaneme s využitím lemmatu 3.23
$$\begin{aligned} \mathbb{q} &= \mathbb{x} - \sum_{i=1}^{h} \alpha_i \mathbb{x}_i \\ \theta = \mathbb{A}\mathbb{q} &= \mathbb{A}\left(\mathbb{x} - \sum_{i=1}^{h} \alpha_i \mathbb{x}_i\right) = \mathbb{A}\mathbb{x} - \sum_{i=1}^{h} \alpha_i \overbrace{(\mathbb{A}\mathbb{x}_i)}^{=\mathbb{y}_i} \, , \end{aligned}$$
tedy $\mathbb{A}\mathbb{x} = \sum_{i=1}^{h} \alpha_i \mathbb{y}_i$ a hledané koeficienty α_i skutečně existují – jsou to souřadnice vektoru $\mathbb{A}\mathbb{x} \in T^{m,1}$ v bázi $(\mathbb{y}_1, \dots, \mathbb{y}_h)$!
- Zbývá ověřit, že součet je direktní, tedy že $P \cap S_0 = \{\theta\}$. Nechť $\mathbb{x} \in T^{n,1}$ je libovolný vektor z tohoto průniku, ukážeme, že nutně $\mathbb{x} = \theta$. Z našeho předpokladu musí platit, že
$$\exists \beta_1, \dots, \beta_h \in T : \ \mathbb{x} = \sum_{i=1}^{h} \beta_i \mathbb{x}_i \quad \wedge \quad \mathbb{A}\mathbb{x} = \theta \, ,$$
což implikuje
$$\theta = \mathbb{A}\mathbb{x} = \sum_{i=1}^{h} \beta_i (\mathbb{A}\mathbb{x}_i) \, .$$
Jelikož je ale soubor vektorů $\mathbb{y}_i = \mathbb{A}\mathbb{x}_i$ lineárně nezávislý a lineární kombinace výše je rovna nulovému vektoru, musí nutně platit $\forall i \in \hat{h} : \ \beta_i = 0$, tedy $\mathbb{x} = \theta$ a důkaz je hotov[26].

$\square$

Poznámka 3.25. *Jak plyne z Frobeniovy věty, je-li matice soustavy $\mathbb{A}$ čtvercová a regulární, existuje pro jakýkoli vektor pravých stran $\mathbb{b}$ právě jedno řešení soustavy $\mathbb{A}\mathbb{x} = \mathbb{b}$. Stačí obě strany rovnice vynásobit zleva inverzní maticí $\mathbb{A}^{-1}$ a dostaneme*

$$\mathbb{x} = \mathbb{A}^{-1}\mathbb{b} \, .$$

[26] Hurá, hurá, třikrát sláva!

Ctěného čtenáře si zde dovolujeme laskavě vyzvat k zopakování definice horního stupňovitého tvaru matice (definice 1.25), další postupy řešení budou pracovat pouze se soustavami $(\mathbb{A} \mid \mathbb{b})$ v tomto tvaru. Definici pro ilustraci doplňme jednoduchým schématem řešitelné soustavy s rozšířenou maticí typu $m \times (n+1)$ o právě h nenulových řádcích, s indexy hlavních sloupců značenými $1 = j_1 < j_2 < \cdots < j_h$.

$$\left(\begin{array}{cccccccccccc|c}
\underbrace{\alpha_{1j_1}}_{\neq 0} & * & * & * & * & * & * & \cdots & * & * & * & * & \beta_1 \\
0 & 0 & 0 & \underbrace{\alpha_{2j_2}}_{\neq 0} & * & * & * & \cdots & * & * & * & * & \beta_2 \\
0 & 0 & 0 & 0 & 0 & \underbrace{\alpha_{3j_3}}_{\neq 0} & * & \cdots & * & * & * & * & \beta_3 \\
\vdots & & \vdots & & & & & & \vdots & & & \vdots & \vdots \\
0 & 0 & 0 & \cdots & & & & \cdots & 0 & \underbrace{\alpha_{hj_h}}_{\neq 0} & * & * & \beta_h \\
0 & 0 & 0 & \cdots & & & & \cdots & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \cdots & & & & \cdots & 0 & 0 & 0 & 0 & 0
\end{array}\right)$$

Řešení homogenní soustavy

Jak známo, každá homogenní soustava je řešitelná. Každý nenulový řádek soustavy s maticí v horním stupňovitém tvaru nám umožňuje spočítat jednu neznámou, a to zpětným výpočtem (postupným dosazováním) odspoda nahoru. Tyto proměnné odpovídají hlavním sloupcům matice a nazýváme je **vázané proměnné**. Ostatní proměnné nazýváme **volné proměnné**. Shrňme si několik jednoduchých faktů:

- Dosadíme-li za všechny volné proměnné konkrétní hodnoty, vázané proměnné lze jednoznačně dopočítat.
- Volných proměnných je přesně $n - h = n - h(\mathbb{A})$, což je podle Frobeniovy věty rovno dimenzi hledaného podprostoru řešení S_0.
- Pokud by nás z každého řešení zajímaly pouze volné proměnné, označme je např. $(t_1, t_2, \ldots, t_{n-h}) \in T^{n-h}$, řešením soustavy by bylo celé T^{n-h}.
- Libovolná lineární kombinace nějakých řešení homogenní soustavy je také jejím řešením.
- Zvolíme-li jakoukoli bázi podprostoru T^{n-h} a pro každý bazický vektor reprezentující nějakou volbu volných proměnných dopočítáme vázané proměnné, dostaneme dle předchozích bodů bázi S_0.

Algoritmus 3.26 (Řešení homogenní SLR)**.** *Řešíme soustavu $\mathbb{A}\mathbb{x} = \theta$ s rozšířenou maticí $(A \mid \theta)$, kde $\mathbb{A} \in T^{m,n}$ je v horním stupňovitém tvaru. Nemá-li zadaná soustava matici v horním stupňovitém tvaru, převedeme ji na něj pomocí GEM (množina řešení se nemění).*

1. *Pokud tím neporušíme horní stupňovitý tvar, můžeme prohodit pořadí sloupců v matici $\mathbb{A}$ (stejně prohodíme i příslušné proměnné).*

2. *Za vázané proměnné označíme proměnné příslušející hlavním sloupcům matice. Zbývající volné proměnné označme např. $(t_1, \ldots, t_{n-h})$.*

3. *Zvolíme libovolnou bázi prostoru T^{n-h}, každá volba volných proměnných je tedy v jejím lineárním obalu*[27].

4. *Pro každý zvolený bazický vektor $(t_1, \ldots, t_{n-h}) \in T^{n-h}$ reprezentující volbu volných proměnných dopočítáme ze soustavy vázané proměnné.*

5. *Dostáváme LN soubor $n-h$ vektorů*[28], *který generuje S_0.*

Příklad 3.27. *Řešme homogenní soustavu s maticí:*

$$\mathbb{A} = \left(\begin{array}{ccccc|c} 1 & 3 & 2 & 0 & 3 & 0 \\ 1 & 1 & 1 & -1 & 5 & 0 \\ 2 & 8 & 5 & 3 & 7 & 0 \\ 3 & 9 & 6 & 2 & 12 & 0 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 3 & 2 & 0 & 3 & 0 \\ 0 & 2 & 1 & 3 & 1 & 0 \\ 0 & 0 & 0 & 2 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Vázané proměnné jsou tedy x_1, x_2, x_4, volné proměnné jsou x_3, x_5.

- *Při volbě $(x_3, x_5) = (1, 0)$ dopočítáme:* $\quad x_4 = 0,\ x_2 = -\frac{1}{2},\ x_1 = -\frac{1}{2}$.
- *Při volbě $(x_3, x_5) = (0, 1)$ dopočítáme:* $\quad x_4 = -\frac{3}{2},\ x_2 = \frac{7}{4},\ x_1 = -\frac{33}{4}$.
- *Dostáváme LN soubor dvou řešení: $(-\frac{1}{2}, -\frac{1}{2}, 1, 0, 0)$ a $(-\frac{33}{4}, \frac{7}{4}, 0, -\frac{3}{2}, 1)$ a tedy platí*
$$S_0 = \langle (-\tfrac{1}{2}, -\tfrac{1}{2}, 1, 0, 0), (-\tfrac{33}{4}, \tfrac{7}{4}, 0, -\tfrac{3}{2}, 1) \rangle \,.$$

Nemusíme ale pro volné proměnné vždy volit standardní bázi. Hrozí-li během dalšího řešení zlomky, můžeme bazické řešení volit i prozíravěji, například

- $(x_3, x_5) = (2, 0) \ \Rightarrow\ x_4 = 0,\ x_2 = -1,\ x_1 = -1,$
- $(x_3, x_5) = (1, 2) \ \Rightarrow\ x_4 = -3,\ x_2 = 3,\ x_1 = -17.$
- *Dostáváme pak jiný tvar množiny řešení,*
$$S_0 = \langle (-1, -1, 2, 0, 0), (-17, 3, 1, -3, 2) \rangle.$$

Následující věta nám dá alternativní metodu řešení homogenní soustavy v případě, kdy jsme pomocí GEM schopni matici soustavy jednoduše převést do ještě speciálnějšího tvaru než jen horního stupňovitého.

[27] V případě standardní báze tedy samozřejmě platí $(t_1, t_2, \ldots, t_{n-h}) \in \langle (1, 0, 0, \ldots, 0, 0), (0, 1, 0, \ldots, 0, 0), \ldots, (0, 0, 0, \ldots, 0, 1) \rangle$.

[28] Lineární nezávislost tohoto souboru si dobře rozmyslete.

Věta 3.28. *Nechť $\mathbb{A} \in T^{m,n}$ a*

$$\mathbb{A} \sim \begin{pmatrix} \mathbb{E} & \mathbb{B} \\ \Theta & \Theta \end{pmatrix},$$

kde $\mathbb{E} \in T^{k,k}$ je jednotková matice, $\mathbb{B} \in T^{k,n-k}$ a symboly Θ značí nulové matice příslušných rozměrů[29]*. Potom řádky matice*

$$(-\mathbb{B}^T \ \mathbb{E}) \in T^{n-k,n},$$

kde $\mathbb{E} \in T^{n-k,n-k}$ je jednotková matice, tvoří bázi prostoru řešení S_0.

Důkaz. Řešme dle algoritmu 3.26 soustavu s maticí

$$\begin{pmatrix} \mathbb{E} & \mathbb{B} \\ \Theta & \Theta \end{pmatrix}.$$

Z tvaru matice je zřejmé, že $(x_1, \ldots, x_k)$ jsou vázané proměnné a $(x_{k+1}, \ldots, x_n)$ volné proměnné. Pokud za bazická řešení pro volné proměnné zvolíme standardní bázi T^{n-k}, pak:

- $(x_{k+1}, \ldots, x_n) = (1, 0, 0, \ldots, 0) \Rightarrow (x_1, \ldots, x_k) = (-\mathbb{B}_{1,1}, -\mathbb{B}_{2,1}, \ldots, -\mathbb{B}_{k,1})$,
- $(x_{k+1}, \ldots, x_n) = (0, 1, 0, \ldots, 0) \Rightarrow (x_1, \ldots, x_k) = (-\mathbb{B}_{1,2}, -\mathbb{B}_{2,2}, \ldots, -\mathbb{B}_{k,2})$
- a dále analogicky. Každé bazické řešení je pak nějakým z řádků matice

$$(-\mathbb{B}^T \ \mathbb{E}) \in T^{n-k,n}.$$

Alternativně lze využít blokového násobení matic (viz definice 3.47 v dodatku na konci této kapitoly). Pak dostáváme

$$\begin{pmatrix} \mathbb{E} & \mathbb{B} \\ \Theta & \Theta \end{pmatrix} \begin{pmatrix} -\mathbb{B} \\ \mathbb{E}^T \end{pmatrix} = \begin{pmatrix} -\mathbb{E}\mathbb{B} + \mathbb{B}\mathbb{E}^T \\ \Theta \end{pmatrix} = \begin{pmatrix} -\mathbb{B} + \mathbb{B} \\ \Theta \end{pmatrix} = \Theta.$$

□

Příklad 3.29. *Ještě jednou si vyřešíme soustavu z příkladu 3.27, pro neznámé $(x_1, x_2, x_3, x_4, x_5)$,*

$$\mathbb{A} = \left(\begin{array}{ccccc|c} 1 & 3 & 2 & 0 & 3 & 0 \\ 1 & 1 & 1 & -1 & 5 & 0 \\ 2 & 8 & 5 & 3 & 7 & 0 \\ 3 & 9 & 6 & 2 & 12 & 0 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 1/2 & 0 & 33/4 & 0 \\ 0 & 1 & 1/2 & 0 & -7/4 & 0 \\ 0 & 0 & 0 & 1 & 3/2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Prohozením třetího a čtvrtého sloupce dostaneme soustavu ve speciálním tvaru, kde neznámé jsou $(x_1, x_2, x_4, x_3, x_5)$:

$$(\mathbb{E} \ \mathbb{B}) = \begin{pmatrix} 1 & 0 & 0 & 1/2 & 33/4 \\ 0 & 1 & 0 & 1/2 & -7/4 \\ 0 & 0 & 1 & 0 & 3/2 \end{pmatrix}$$

[29] Jedna je typu $(m-k) \times k$, druhá je typu $(m-k) \times (n-k)$.

a

$$(-\mathbb{B}^T\ \mathbb{E}) = \begin{pmatrix} -1/2 & -1/2 & 0 & 1 & 0 \\ -33/4 & 7/4 & -3/2 & 0 & 1 \end{pmatrix}.$$

Nyní opět prohodíme třetí a čtvrtý sloupec a získáme hledanou bázi množiny S_0:

$$S_0 = \langle(-\tfrac{1}{2}, -\tfrac{1}{2}, 1, 0, 0), (-\tfrac{33}{4}, \tfrac{7}{4}, 0, -\tfrac{3}{2}, 1)\rangle\,.$$

Řešení nehomogenní soustavy

Z Frobeniovy věty i dříve odvozených výsledků víme, že platí

$$S = \tilde{\mathbb{x}} + S_0\,,$$

kde $\tilde{\mathbb{x}}$ je jakékoli řešení soustavy $\mathbb{A}\mathbb{x} = \mathbb{b}$. Stačí tedy toto řešení (tzv. partikulární) najít a pak suše konstatovat, že zbytek problému je už „jen“ kompletní vyřešení homogenní rovnice, a to už přece umíme.

Algoritmus 3.30 (Řešení SLR)**.** *Řešíme soustavu $\mathbb{A}\mathbb{x} = \mathbb{b}$ s rozšířenou maticí $(A \mid \mathbb{b})$, kde $\mathbb{A} \in T^{m,n}$ je v horním stupňovitém tvaru. Nemá-li zadaná soustava matici v horním stupňovitém tvaru, převedeme ji na něj pomocí GEM (množina řešení se nemění).*

1. *Pokud tím neporušíme horní stupňovitý tvar, můžeme prohodit pořadí sloupců v matici $\mathbb{A}$ (stejně prohodíme i příslušné proměnné).*

2. *Pokud $h(\mathbb{A}) < h(\mathbb{A} \mid \mathbb{b})$, řešení neexistuje. V opačném případě postupujeme dále.*

3. *Za vázané proměnné označíme proměnné příslušející hlavním sloupcům matice. Zbývající volné proměnné označíme $(t_1, \ldots, t_{n-h})$.*

4. *Pro nalezení $\tilde{\mathbb{x}}$ zvolme za $(t_1, \ldots, t_{n-h})$ libovolně[30] a ze soustavy $(\mathbb{A} \mid \mathbb{b})$ dopočítejme vázané proměnné.*

5. *Pro nalezení S_0 zvolíme libovolnou bázi prostoru T^{n-h} (různé volby pro volné proměnné). Přejdeme k řešení přidružené homogenní rovnice, tedy **vynulujeme** pravou stranu soustavy.*

6. *Pro každý zvolený bazický vektor $(t_1, \ldots, t_{n-h}) \in T^{n-h}$ reprezentující volbu volných proměnných dopočítáme ze soustavy $(\mathbb{A} \mid \theta)$ vázané proměnné a dostáváme bázi S_0.*

7. *Řešením je $S = \tilde{\mathbb{x}} + S_0$.*

Příklad 3.31. *Soustavu s maticí uvedenou v předchozích příkladech doplníme o pravou stranu. Řádkovými úpravami GEM upravíme rozšířenou matici:*

$$\left(\begin{array}{ccccc|c} 1 & 3 & 2 & 0 & 3 & 3 \\ 1 & 1 & 1 & -1 & 5 & -2 \\ 2 & 8 & 5 & 3 & 7 & 13 \\ 3 & 9 & 6 & 2 & 12 & 11 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 1/2 & 0 & 33/4 & -3 \\ 0 & 1 & 1/2 & 0 & -7/4 & 2 \\ 0 & 0 & 0 & 1 & 3/2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

[30] Oblíbenou volbou je pochopitelně $(t_1, \ldots, t_{n-h}) = (0, \ldots, 0)$, ale není to jediná možnost.

Pro volbu volných proměnných $(x_3, x_5) = (0, 0)$ dostáváme pro vázané proměnné (x_1, x_2, x_4) soustavu

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

a partikulární řešení je $(-3, 2, 0, 1, 0)$. S využitím znalosti S_0 z příkladu 3.27 dostáváme množinu všech řešení například ve tvaru

$$S = (-3, 2, 0, 1, 0) + \langle(-1, -1, 2, 0, 0), (-33, 7, 0, -6, 4)\rangle.$$

Jak již mohlo přirozeně vyplynout jak z uvedených příkladů, tak z vyložených postupů, množina řešení obecné SLR nemá jednoznačný popis. Řeší-li více lidí tutéž soustavu rovnic, mohou dospět k velmi odlišně „vypadajícím“ množinám řešení. Stačí, pokud při GEM volí odlišnou posloupnost elementárních úprav. I se stejným horním stupňovitým tvarem matice soustavy se lze odchýlit, například jinou volbou volných proměnných nebo volbou jiných bazických řešení.

Chceme-li ověřit rovnost dvou množin tvaru $\mathbb{x} + S_0$, můžeme opět použít pojem hodnost a navázat tak na přehled *Metody výpočtů (nejen) hodnosti* v části 3.2.

Pozorování 3.32. *Nechť $u, v, y_1, \dots, y_k, z_1, \dots, z_k \in T^n$, kde soubory $(y_1, \dots, y_k)$ a $(z_1, \dots, z_k)$ jsou LN. Rovnost*

$$u + \langle y_1, \dots, y_k\rangle = v + \langle z_1, \dots, z_k\rangle \tag{3.6}$$

platí právě tehdy, když matice, jejíž řádky tvoří vektory

$$y_1, \dots, y_k, z_1, \dots, z_k, u - v$$

má hodnost rovnu k.

Důkaz.
$(\Rightarrow)$: Platí-li (3.6), pak $u - v + \langle y_1, \dots, y_k\rangle = \langle z_1, \dots, z_k\rangle$. Z rovnosti rovnou plyne, že $u - v \in \langle y_1, \dots, y_k\rangle$ a oba lineární obaly se rovnají. Tedy platí

$$\langle y_1, \dots, y_k, z_1, \dots, z_k, u - v\rangle = \langle y_1, \dots, y_k\rangle$$

a dimenze obou těchto obalů je rovna k.

$(\Leftarrow)$: Nechť matice, jejíž řádky tvoří vektory $y_1, \dots, y_k, z_1, \dots, z_k, u - v$, má hodnost rovnu k. Protože soubor $(y_1, \dots, y_k)$ je LN, musí

$$u - v \in \langle y_1, \dots, y_k\rangle,$$

tedy platí

$$\langle y_1, \dots, y_k\rangle = \langle u - v, y_1, \dots, y_k\rangle.$$

Dále protože

$$\dim\langle y_1, \dots, y_k\rangle = \dim\langle z_1, \dots, z_k\rangle = \dim\langle y_1, \dots, y_k, z_1, \dots, z_k, u - v\rangle = k,$$

dostáváme z pozorování 2.64 o rovnosti lineárních obalů rovnost

$$\langle u - v, y_1, \dots, y_k \rangle = \langle z_1, \dots, z_k \rangle.$$

Celkem máme

$$u - v + \langle y_1, \dots, y_k \rangle \subseteq \langle u - v, y_1, \dots, y_k \rangle = \langle z_1, \dots, z_k \rangle.$$

Analogicky bychom odvodili druhou inkluzi, neboť oba vektory u,v a oba soubory $(y_1, \dots, y_k)$ a $(z_1, \dots, z_k)$ vystupují v tvrzení zcela symetricky.

Nakonec si stačí uvědomit, že rovnost

$$u + \langle y_1, \dots, y_k \rangle = v + \langle z_1, \dots, z_k \rangle$$

platí právě tehdy, když

$$u - v + \langle y_1, \dots, y_k \rangle = \langle z_1, \dots, z_k \rangle. \qquad \square$$

Příklad 3.33. *Při řešení soustavy v $\mathbb{R}^4$ s maticí*

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

lze různými postupy dospět například k řešením ve tvaru

$$\begin{aligned} S_1 &= (\tfrac{1}{5}, \tfrac{2}{5}, 0, 0) + \langle (2, -1, 5, 0), (1, 2, 0, 5) \rangle, \\ S_2 &= (0, 0, 0, -1) + \langle (0, -5, 5, -10), (3, 1, 5, 5) \rangle. \end{aligned}$$

To, že se tyto množiny rovnají[31]*, ověříme výpočtem hodnosti matice sestavené podle pozorování 3.32,*

$$\begin{pmatrix} 2 & -1 & 5 & 0 \\ 1 & 2 & 0 & 5 \\ 0 & -5 & 5 & -10 \\ 3 & 1 & 5 & 5 \\ \frac{1}{5} & \frac{2}{5} & 0 & 1 \end{pmatrix},$$

která se skutečně rovná

$$\dim\langle (2, -1, 5, 0), (1, 2, 0, 5) \rangle = \dim\langle (0, -5, 5, -10), (3, 1, 5, 5) \rangle = 2\,.$$

3.5 Lineární variety

Zdůrazněme, že se v této části omezíme na jediný typ vektorových prostorů, a to na $V = T^n$.

[31] Pozor, ověřujeme jen rovnost $S_1 = S_2$, nejedná se ale o zkoušku správnosti řešení soustavy. Pouze takto zjistíme, že jsou oba výsledky buďto stejně dobře, nebo „stejně špatně“!

Dvě interpretace SLR

Než přejdeme k definování pojmu *lineární varieta*, vrátíme se ještě o krok zpět a zamyslíme se, jak lze soustavy lineárních rovnic různě interpretovat. Nabízí se minimálně dva různé pohledy, jeden „sloupcový“ (se kterým jsme už měli tu čest při důkazu první části Frobeniovy věty 3.24) a druhý „řádkový“ (analogický k motivačnímu úvodu v první kapitole, kde jsme soustavu rovnic v $\mathbb{R}^2$ nebo $\mathbb{R}^3$ interpretovali jako **průnik** přímek či rovin).

Pozorování 3.34. *Soustavu lineárních rovnic $\mathbb{A}\mathbb{x} = \mathbb{b}$, $\mathbb{A} \in T^{m,n}$ lze interpretovat sloupcově následujícím způsobem:*

Vztah $\mathbb{A}\mathbb{x} = \mathbb{b}$ lze přepsat jako

$$\forall i \in \hat{m} : \sum_{j=1}^{n} \alpha_{ij} x_j = \beta_i$$

a dále jako

$$x_1 \begin{pmatrix} \alpha_{11} \\ \alpha_{21} \\ \vdots \\ \alpha_{m1} \end{pmatrix} + x_2 \begin{pmatrix} \alpha_{12} \\ \alpha_{22} \\ \vdots \\ \alpha_{m2} \end{pmatrix} + \cdots + x_n \begin{pmatrix} \alpha_{1n} \\ \alpha_{2n} \\ \vdots \\ \alpha_{mn} \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_m \end{pmatrix}.$$

Opětovným zjednodušením zápisu dostáváme

$$\sum_{j=1}^{n} x_j \mathbb{A}_{:j} = \mathbb{b}\,,$$

*tedy platí, že složky řešení $x_1, \ldots, x_n$ jsou vlastně koeficienty v takové lineární kombinaci **sloupců** matice $\mathbb{A}$, která je rovna vektoru pravé strany $\mathbb{b}$.*

Pozorování 3.35. *Soustavu lineárních rovnic $\mathbb{A}\mathbb{x} = \mathbb{b}$, $\mathbb{A} \in T^{m,n}$ lze interpretovat řádkově následujícím způsobem:*

*Každý **řádek** matice soustavy představuje jednu lineární rovnici. Množina řešení každé takové rovnice*

$$\alpha_{i1} x_1 + \cdots + \alpha_{in} x_n = \beta_i$$

(pokud je alespoň jeden z koeficientů α_{ij} nenulový[32]) je množina bodů v T^n, kterou si lze geometricky představit[33]. V případě $\mathbb{R}^2$ je to přímka, v případě $\mathbb{R}^3$ rovina. Pro obecné T^n si již brzy zavedeme pojem nadrovina, *neboli podprostor dimenze $n-1$ posunutý z počátku do nějakého bodu.*

*Jelikož v soustavě musí všechny rovnice platit současně, hledáme při jejím řešení **průnik** jednotlivých nadrovin.*

[32] A co když jsou všechny α_{ij} v nějakém řádku nulové, co platí pak?

[33] Alespoň v omezené míře, že ano…

Definice lineární variety

Pod pojmem *lineární varieta* budeme rozumět libovolný podprostor „posunutý“ z počátku θ o nějaký vektor.

Definice 3.36. *Neprázdnou množinu $W \subseteq V$ nazveme **lineární varietou** (případně pouze **varietou**), pokud existují $a \in W$ a $P \subset\subset V$ takové, že*

$$W = a + P.$$

*Podprostor P nazýváme **zaměřením** variety W a značíme ho $Z(W)$.*

- *Číslo $\dim Z(W)$ nazýváme **dimenzí** variety W,*
- *je-li $\dim V = n \in \mathbb{N}$, pak číslo $n - \dim Z(W)$ nazýváme **kodimenzí** variety W,*
- *každý nenulový vektor z $Z(W)$ nazýváme **směrovým vektorem** variety W,*
- *každý vektor a takový, že $W = a + Z(W)$, nazýváme **vektorem posunutí** variety W.*

Věta 3.37. *Buď W lineární varieta.*

(i) Každý její vektor je současně vektorem posunutí, tj. $\forall a \in W: \ W = a + Z(W)$.

(ii) Zaměření variety $Z(W)$ je určeno jednoznačně.

Důkaz. (i) Nechť $W = a + Z(W)$. Pak pro libovolné $b \in W$ existuje $x \in Z(W)$ tak, že $b = a + x$. Odkud dostáváme, že $b - a = x \in Z(W)$.

Protože je $Z(W)$ podprostor, platí

$$(b - a) + Z(W) = Z(W).$$

Pro libovolné $b \in W$ tedy dostáváme

$$\begin{aligned} W &= a + Z(W) \\ &= a + (b - a) + Z(W) \\ &= b + Z(W), \end{aligned}$$

tedy $b \in W$ je také vektorem posunutí variety W.

(ii) Existují-li dva podprostory $P, Q \subset\subset V$ takové, že

$$W = a + P = a + Q,$$

dostaneme ihned z poslední rovnosti, že $P = Q$.

□

Definice 3.38. *Nechť $V = T^n$ je libovolný.*

- *Varietu o dimenzi 0 nazýváme **bod**.*

- *Varietu o dimenzi* 1 *nazýváme* ***přímka****.*
- *Varietu o dimenzi* 2 *nazýváme* ***rovina****.*
- *Varietu o kodimenzi* 1 *nazýváme* ***nadrovina****.*

Příklad 3.39. *Jak všichni dobře víme, množina bodů* $W_1 = \{(x, y) \mid y = 2x + 1\}$ *představuje přímku v* $\mathbb{R}^2$*. To je v souladu i s naší obecnější definicí, kde můžeme volit*

$$a = (0, 1) \quad a \quad Z(W_1) = \langle(1, 2)\rangle.$$

Potom skutečně

$$a + Z(W_1) = (0, 1) + \langle(1, 2)\rangle = \{(t, 1 + 2t) \mid t \in \mathbb{R}\} = W_1.$$

Podobně, množina $W_2 = \{(x, y, z) \mid x + y + z = 1\}$ *představuje rovinu v* $\mathbb{R}^3$*. I zde najdeme vyjádření v souladu s definicemi 3.36 a 3.38. Pokud*

$$a = (1, 0, 0) \quad a \quad Z(W_2) = \langle(-1, 1, 0), (-1, 0, 1)\rangle,$$

pak platí

$$a + Z(W_2) = (1, 0, 0) + \langle(-1, 1, 0), (-1, 0, 1)\rangle = \{(1 - s - t, s, t) \mid s, t \in \mathbb{R}\} = W_2.$$

Příklad 3.40. *Poněkud méně intuitivní význam pojmů přímka či rovina dostaneme v případě VP nad konečnými tělesy:*

- *Množina*

  $$W_3 = (1, 0, 0, 0) + \langle(1, 1, 1, 1)\rangle = \{(1 + t, t, t, t) \mid t \in T\}$$

  je přímka v každém T^4*, tedy* $\{(1, 0, 0, 0), (2, 1, 1, 1), (0, 2, 2, 2)\}$ *je přímkou v* $\mathbb{Z}_3^4$*.*

- *Množina*

  $$W_4 = (1, 1, 0, 0) + \langle(0, 1, 1, 0), (1, 0, 0, 1)\rangle = \{(1 + t, 1 + s, s, t) \mid s, t \in T\}$$

  je rovina v každém T^4*, tedy* $\{(1, 1, 0, 0), (1, 0, 1, 0), (0, 1, 0, 1), (0, 0, 1, 1)\}$ *je rovinou v* $\mathbb{Z}_2^4$*.*

Z Frobeniovy věty i předchozích poznatků ($S = \tilde{\mathbb{x}} + S_0$) už víme, že každá řešitelná soustava lineárních rovnic určuje svými řešeními lineární varietu. Tato korespondence platí i druhým směrem, jak si hned dokážeme – tedy ke každé lineární varietě existuje nějaká SLR, kterou právě všechny vektory z této lineární variety řeší.

Věta 3.41. *Nechť* $M \subseteq V = T^n$ *je neprázdná. Pak* M *je lineární varietou právě tehdy, když existuje soustava lineárních rovnic* $\mathbb{A}\mathbb{x} = \mathbb{b}$*, jejíž množinou řešení je* M*. Navíc platí*

$$h(\mathbb{A}) = n - \dim M\,.$$

Důkaz. Fakt, že množina řešení každé (řešitelné) SLR je lineární varieta, již známe. Dokážeme opačnou implikaci ($\Rightarrow$):

Nechť $M \neq \emptyset$ je lineární varieta, tedy

$$M = a + P\,,$$

kde $a \in V$, $P \subset\subset V$ a $\dim P = k \in \{0, 1, \ldots, n\}$. Rozlišíme tři případy:

1. Nechť $k = n$, tedy $M = V$. Celý prostor V je zjevně množinou řešení triviální soustavy $\Theta\mathbb{x} = \theta$.

2. Nechť $k = 0$, tedy $M = a + P = a + \{\theta\} = \{a\}$. Tato jednoprvková množina je řešením soustavy s maticí $\mathbb{A} = \mathbb{E}$, tedy $\mathbb{E}\mathbb{x} = \mathbb{a}$, kde $\mathbb{a}$ je $n$tice $a \in T^n$ zapsaná do sloupce.

3. Nechť $\dim P = k \in \widehat{n-1}$, označme jako $(y_1, \ldots, y_k)$ nějakou bázi P. Najdeme matici $\mathbb{A} \in T^{n-k,n}$ a vektor $\mathbb{b} \in T^{n-k,1}$ takové, že $M = a + \langle y_1, \ldots, y_k \rangle$ je množina řešení soustavy $\mathbb{A}\mathbb{x} = \mathbb{b}$. Napíšeme-li vektory $(y_1, \ldots, y_k)$ popořadě do sloupců matice, označme ji $\mathbb{Y} \in T^{n,k}$, musí platit

   $$\mathbb{A}\mathbb{Y} = \Theta \in T^{n-k,k}\text{[34]}\,,$$

   nicméně neznámými jsou zde pro nás prvky matice $\mathbb{A} = (\alpha_{ij})_{i \in \hat{m}, j \in \hat{n}}$, kterou chceme najít. S využitím transpozice matic a pravidla pro transpozici součinu vztah upravíme na

   $$\mathbb{Y}^T\mathbb{A}^T = \Theta \in T^{k,n-k}\,.$$

   Z tohoto plyne, že každý sloupec matice $\mathbb{A}^T$ (a tedy každý řádek původní matice $\mathbb{A}$!) je nějakým řešením homogenní soustavy

   $$\mathbb{Y}^T\mathbb{x} = \theta\,.$$

   Jelikož z předpokladu $h(\mathbb{Y}^T) = h(\mathbb{Y}) = k$, Frobeniova věta 3.24 implikuje, že existuje $(n-k)$prvkový LN soubor řešení této soustavy $\mathbb{Y}^T\mathbb{x} = \theta$. Tento soubor stačí napsat po řádcích do matice a dostáváme hledanou $\mathbb{A} \in T^{n-k,n}$.

   Máme tedy zajištěno, že podprostor P je množinou řešení S_0 homogenní soustavy s maticí $\mathbb{A}$, je třeba ještě „vyladit“ sloupec pravých stran $\mathbb{b}$ tak, aby vektor posunutí variety a byl partikulárním řešením hledané soustavy $(\mathbb{A} \mid \mathbb{b})$. To je ale jednoduché, napíšeme-li vektor a do sloupce (označme $\mathbb{a}$), pravou stranu $\mathbb{b}$ získáme jednoduchým vynásobením – musí totiž platit vztah

   $$\mathbb{A}\mathbb{a} = \mathbb{b}\,.$$

Vztah $h(\mathbb{A}) = n - \dim M$ plyne přímo z Frobeniovy věty 3.24 a předchozích bodů v důkazu. $\square$

Jednoduchý důsledek získáme použitím předchozí věty ve speciálním případě $\dim P = n - 1$.

[34] Uvědomit si, jakých rozměrů jsou používané matice, nikdy neuškodí.

Důsledek 3.42. *Množina $M \subseteq V = T^n$ je nadrovinou právě když je množinou řešení jedné lineární rovnice*

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = \beta\,,$$

kde alespoň jeden z koeficientů $\alpha_1, \ldots, \alpha_n$ je nenulový.

Parametrické a neparametrické rovnice variety

Definice 3.43. *Nechť $W \subseteq V = T^n$ je lineární varieta, označme bázi $Z(W)$ jako $(a_1, \ldots, a_k)$.*

- *Vztah $W = a + \langle a_1, \ldots, a_k\rangle$ lze vyjádřit jako*

  $$u \in W \Leftrightarrow \exists \alpha_1, \ldots, \alpha_n \in T:\ u = a + \sum_{i=1}^{k} \alpha_i a_i\,.$$

  Parametrickými rovnicemi *variety W rozumíme rovnici*

  $$u = a + \sum_{i=1}^{k} \alpha_i a_i$$

  rozepsanou po složkách, tedy pro $u = (x_1, \ldots, x_n) \in T^n$.

- ***Neparametrickými rovnicemi*** *variety W rozumíme po složkách (pro $u = (x_1, \ldots, x_n) \in T^n$) rozepsanou soustavu lineárních rovnic*

  $$\mathbb{A}\mathbb{x} = \mathbb{b}$$

  určující varietu W.

Odvodíme si parametrické rovnice přímek a rovin v $\mathbb{R}^3$. Čtenáře, který je vybaven alespoň základy středoškolské analytické geometrie, jistě odvozené parametrické rovnice nepřekvapí.

- Je-li W přímka, lze ji charakterizovat rovnicí

  $$u = a + \alpha b,$$

  kde $a \in W$ a zaměření W je $\langle b\rangle$.

  Rozepíšeme-li vektory výše po složkách, $u = (x, y, z)$, $a = (a_1, a_2, a_3)$ a $b = (b_1, b_2, b_3)$, dostaneme parametrické rovnice přímky,

  $$\begin{aligned} x &= a_1 + \alpha b_1 \\ y &= a_2 + \alpha b_2 \\ z &= a_3 + \alpha b_3\,, \end{aligned}$$

  kde $\alpha \in \mathbb{R}$.

- Je-li W rovina, lze ji charakterizovat rovnicí

  $$u = a + \alpha b + \beta c,$$

  kde $a \in W$ a zaměření W je $\langle b, c \rangle$.

  Rozepíšeme-li vektory výše po složkách, $u = (x, y, z)$, $a = (a_1, a_2, a_3)$, $b = (b_1, b_2, b_3)$ a $c = (c_1, c_2, c_3)$, dostaneme parametrické rovnice roviny,

  $$\begin{aligned} x &= a_1 + \alpha b_1 + \beta c_1 \\ y &= a_2 + \alpha b_2 + \beta c_2 \\ z &= a_3 + \alpha b_3 + \beta c_3 \, , \end{aligned}$$

  kde $\alpha, \beta \in \mathbb{R}$.

Základním typem úlohy, se kterým se v kurzu můžeme setkat, je převádění variet zadaných v jednom z vyložených dvou tvarů do druhého. Převod **z neparametrických rovnic na parametrické** ani nemusíme nijak rozebírat, stačí totiž vyřešit zadanou soustavu $\mathbb{A}\mathbb{x} = \mathbb{b}$ a množinu řešení zapsat dle definice 3.43. Druhý směr převodu, **z parametrických rovnic na neparametrické**, se v podstatě řídí postupem důkazu věty 3.41, heslovitě si jej tady ještě zopakujeme.

Algoritmus 3.44 (Převod parametricky zadané variety na neparametrický tvar)**.** *Máme zadanou lineární varietu $W = a + P$ o dimenzi $\dim W = k$. Hledáme soustavu lineárních rovnic $\mathbb{A}\mathbb{x} = \mathbb{b}$ s maticí $(\mathbb{A} \mid \mathbb{b})$, jejíž množinou všech řešení je právě W.*

1. *Je-li $k = 0$, pak hledanou soustavou je $(\mathbb{E} \mid \mathbb{a})$, kde $\mathbb{a}$ je vektor a zapsaný do sloupce. Je-li $k = n$, hledanou soustavou je $(\Theta \mid \theta)$.*
2. *Pro $k \in \widehat{n-1}$ označme bázi P jako $(y_1, \dots, y_k)$ a vyřešme homogenní soustavu $(\widetilde{\mathbb{Y}} \mid \theta)$ kde matice $\widetilde{\mathbb{Y}}$ obsahuje ve svých řádcích vektory $y_1, \dots, y_k$.*
3. *Hledanou matici $\mathbb{A}$ po řádcích sestavíme z vektorů libovolné báze řešení $(\widetilde{\mathbb{Y}} \mid \theta)$.*
4. *Hledaný vektor $\mathbb{b}$ získáme vynásobením $\mathbb{A}\mathbb{a} = \mathbb{b}$.*

Příklad 3.45. *Nalezneme parametrické rovnice variety W v $\mathbb{R}^4$ zadané rovnicemi*

$$\begin{aligned} x + y - z + u &= 1 \\ 2x \qquad\quad + u &= 2 \end{aligned} \, .$$

Varieta W má dimenzi rovnou hodnosti příslušné matice soustavy,

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

Tedy $\dim W = 2$ a jedná se o rovinu v $\mathbb{R}^4$.

Množina řešení soustavy získaná standardním postupem je tvaru

$$W = (1, 0, 0, 0) + \langle (1, 1, 0, -2), (0, 1, 1, 0) \rangle.$$

Vektory $(1,1,0,-2),(0,1,1,0)$ *jsou směrové vektory roviny* W *a parametrické rovnice jsou*

$$\begin{array}{rcrcrcr} x & = & 1 & + & s & & \\ y & = & & & s & + & t \\ z & = & & & & & t \\ u & = & & - & 2s & & \end{array}$$

kde $s,t,\in\mathbb{R}$.

Příklad 3.46. *Nalezneme neparametrické rovnice roviny v* $\mathbb{R}^4$*, která prochází body* $(1,2,1,0)$*,* $(2,3,2,1)$ *a* $(3,2,4,0)$.

Potřebujeme najít jeden vektor posunutí $a\in W$ *a dva směrové vektory, které svým lineárním obalem určí zaměření* $Z(W)$*. Dva směrové vektory dostaneme jako rozdíl dvou různých dvojic zadaných bodů, například*

$$s_1=(2,3,2,1)-(1,2,1,0)=(1,1,1,1)\,,$$
$$s_2=(3,2,4,0)-(1,2,1,0)=(2,0,3,0)\,.$$

Jelikož nejsou jeden násobek druhého, jejich soubor je LN a zadaná trojice bodů proto neleží v jedné přímce.

Vektor posunutí můžeme volit jako libovolný bod variety, například $(1,2,1,0)$*, a proto parametrické rovnice* W *jsou*

$$\begin{array}{rcrcrcr} x & = & 1 & + & s & + & 2t \\ y & = & 2 & + & s & & \\ z & = & 1 & + & s & + & 3t \\ u & = & & & s & & \end{array}$$

kde $s,t\in\mathbb{R}$.

Naším cílem je tedy nalézt matici $\mathbb{A}\in\mathbb{R}^{2,4}$ *a vektor* $\mathbb{b}\in\mathbb{R}^{2,1}$ *takové, aby množina*

$$(1,2,1,0)+\langle(1,1,1,1),(2,0,3,0)\rangle$$

byla množina řešení soustavy $\mathbb{A}\mathbb{x}=\mathbb{b}$.

Dle algoritmu 3.44 *vyřešíme homogenní soustavu s maticí*

$$\left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 2 & 0 & 3 & 0 & 0 \end{array}\right)\sim\left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 0 & -2 & 1 & -2 & 0 \end{array}\right)\,. \tag{3.7}$$

Báze množiny řešení soustavy (3.7) *je například* $((0,-1,0,1),(-3,1,2,0))$*, a proto hledaná matice* $\mathbb{A}$ *je*

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

Vektor pravých stran pak snadno získáme součinem

$$\mathbb{b}=\begin{pmatrix} 0 & -1 & 0 & 1 \\ -3 & 1 & 2 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 2 \\ 1 \\ 0 \end{pmatrix}=\begin{pmatrix} -2 \\ 1 \end{pmatrix}\,.$$

Neparametrické rovnice variety W *jsou tedy* $\mathbb{A}\mathbb{x}=\mathbb{b}$*, což po dosazení dává dvě rovnice v* $\mathbb{R}^4$:

$$\begin{aligned} -y \phantom{{}+2z} + u &= -2 \\ -3x + y + 2z \phantom{{}+u} &= 1\,. \end{aligned}$$

3.6 Dodatky

Blokové násobení a algoritmy pro maticové násobení

Definice 3.47. *Uvažujme dvě matice sestavené po blocích takto:*

$$\mathbb{A} = \begin{pmatrix} \mathbb{A}_{1,1} & \mathbb{A}_{1,2} \\ \mathbb{A}_{2,1} & \mathbb{A}_{2,2} \end{pmatrix}, \qquad \mathbb{B} = \begin{pmatrix} \mathbb{B}_{1,1} & \mathbb{B}_{1,2} \\ \mathbb{B}_{2,1} & \mathbb{B}_{2,2} \end{pmatrix}.$$

Nechť jednotlivé bloky jsou takového typu, že násobení $\mathbb{A}_{i,j}\mathbb{B}_{j,k}$ je definováno pro všechna $i, j, k \in \hat{2}$. Potom platí

$$\mathbb{A}\mathbb{B} = \begin{pmatrix} \mathbb{A}_{1,1}\mathbb{B}_{1,1} + \mathbb{A}_{1,2}\mathbb{B}_{2,1} & \mathbb{A}_{1,1}\mathbb{B}_{1,2} + \mathbb{A}_{1,2}\mathbb{B}_{2,2} \\ \mathbb{A}_{2,1}\mathbb{B}_{1,1} + \mathbb{A}_{2,2}\mathbb{B}_{2,1} & \mathbb{A}_{2,1}\mathbb{B}_{1,2} + \mathbb{A}_{2,2}\mathbb{B}_{2,2} \end{pmatrix}.$$

Poznamenejme, že analogický výsledek platí i pro jinak vytvořené bloky. Například platí

$$\mathbb{A}(\mathbb{B}_1\ \mathbb{B}_2\ \ldots\ \mathbb{B}_p) = (\mathbb{A}\mathbb{B}_1\ \mathbb{A}\mathbb{B}_2\ \ldots\ \mathbb{A}\mathbb{B}_p).$$

Uvažujme čtvercové matice $\mathbb{A}, \mathbb{B} \in T^{n,n}$. K výpočtu součinu $\mathbb{A}\mathbb{B}$ podle definice potřebujeme n^3 operací (operací myslíme vynásobení dvou čísel, které je výpočetně náročnější než sčítání)[35]. Nedalo by se ušetřit?

Rekurzivní algoritmus násobení matic: Vychází z blokového násobení (definice 3.47). Pro jednoduchost výpočtu složitosti předpokládejme, že rozměr matic $n = 2^k$, pro nějaké $k \in \mathbb{N}$. Pokud násobíme dvě matice blokově, dle definice musíme provést dohromady 8 součinů (tvaru $\mathbb{A}_{i,j}\mathbb{B}_{j,k}$) matic polovičních rozměrů (plus nějaké to sčítání, které zanedbáváme). Počet operací násobení označme $F(n)$, potom platí:[36]

$$\begin{aligned} F(n) =& 8F(n/2) = 8(8F(n/4)) = 8(8(8F(n/8))) = \cdots \\ =& 8^k F(n/2^k) = 8^k F(1) = 8^k = (2^k)^3 = \\ =& n^3. \end{aligned}$$

Rekurzivní Strassenův algoritmus: Vychází z blokového násobení, ale vystačí jen se sedmi součiny. Položíme-li

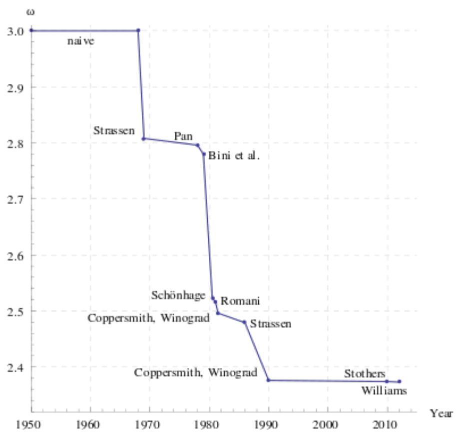
$$\begin{aligned} \mathbb{X}_1 &= (\mathbb{A}_1 + \mathbb{A}_4)(\mathbb{B}_1 + \mathbb{B}_4), & \mathbb{X}_5 &= (\mathbb{A}_1 + \mathbb{A}_2)\mathbb{B}_4, \\ \mathbb{X}_2 &= (\mathbb{A}_3 + \mathbb{A}_4)\mathbb{B}_1, & \mathbb{X}_6 &= (\mathbb{A}_3 - \mathbb{A}_1)(\mathbb{B}_1 + \mathbb{B}_2), \\ \mathbb{X}_3 &= \mathbb{A}_1(\mathbb{B}_2 - \mathbb{B}_4), & \mathbb{X}_7 &= (\mathbb{A}_2 - \mathbb{A}_4)(\mathbb{B}_3 + \mathbb{B}_4), \\ \mathbb{X}_4 &= \mathbb{A}_4(\mathbb{B}_3 - \mathbb{B}_1)\,. \end{aligned}$$

potom platí rovnost

$$\begin{pmatrix} \mathbb{A}_1 & \mathbb{A}_2 \\ \mathbb{A}_3 & \mathbb{A}_4 \end{pmatrix} \begin{pmatrix} \mathbb{B}_1 & \mathbb{B}_2 \\ \mathbb{B}_3 & \mathbb{B}_4 \end{pmatrix} = \begin{pmatrix} \mathbb{X}_1 + \mathbb{X}_4 - \mathbb{X}_5 + \mathbb{X}_7 & \mathbb{X}_3 + \mathbb{X}_5 \\ \mathbb{X}_2 + \mathbb{X}_4 & \mathbb{X}_1 - \mathbb{X}_2 + \mathbb{X}_3 + \mathbb{X}_6 \end{pmatrix}.$$

[35] Je to takový přibližný odhad, součin $\mathbb{A}\mathbb{B}$ má n^2 prvků, pro každý z nich počítáme sumu n sčítanců a pro každý z nich potřebujeme jedno násobení.

[36] Jako by se nechumelilo, jen tak si tu řešíme jeden z mnoha druhů rekurentní rovnic. Děláme to ovšem docela dřevorubecky a bez pořádného vysvětlování! Ctihodný čtenář nechť v tom vidí něžnou reklamu na předmět BI-ZDM.



Obrázek 3.1: Výpočetní složitosti algoritmů pro maticové násobení [zdroj: wikipedia.org]

Pro počet operací $F(n)$, kde opět pro jednoduchost předpokládáme $n = 2^k$, nyní dostáváme lepší odhad:

$$\begin{aligned}F(n) =& 7F(n/2) = 7(7F(n/4)) = 7(7(7F(n/8))) = \cdots \\ =& 7^k F(n/2^k) = 7^k F(1) = 7^k = 7^{\log_2 n} = \qquad [37] \\ =& n^{\log_2 7} \cong n^{2,807}.\end{aligned}$$

Dnes nejvýkonnější algoritmus pro maticové násobení je od Vassilevska Williams (publ. květen 2012), který počítá s přibližně $\mathbf{n^{2,3727}}$ operacemi.

[37] Proč předposlední rovnost $7^{\log_2 n} = n^{\log_2 7}$ vůbec platí? Schválně si trochu procvičte úpravy mocnin.

Kapitola 4

Lineární kódy

V této kapitole si ukážeme aplikaci lineární algebry v teorii kódování. Ukážeme si, že s využitím pojmů z předchozích kapitol umíme zavést dobře fungující a velice obecný „framework“ pro vytváření tzv. *samoopravovacích kódů*.

Kódování, tak jak si jej definujeme, je velice obecný pojem: jedná se o sadu přepisovacích pravidel, díky kterým umíme přepsat jeden řetězec znaků (neboli slovo) z nějaké abecedy na jiný řetězec znaků z jiné či stejné abecedy. Např. UTF8, ASCII, cp1250 jsou příklady kódování, které nám dovoluje zapsat znaky „lidských“ abeced do řetězců nad binární abecedou $\{0, 1\}$. Z matematického pohledu se jedná ale o celkem nezajímavé struktury: prostě je to tabulka přepisovacích pravidel, která jednoznačně dovoluje převody tam a zpátky a nic víc.

O něco zajímavější je situace, kde na kódování začneme klást nějaké požadavky, např. aby zakódovaný text byl co nejkratší. Např. ASCII takové ambice zjevně nemá: všechny znaky, které umí zakódovat, kóduje osmi (resp. sedmi) bity. Přitom by asi bylo z pohledu šetření místa efektivnější, kdyby se např. extrémně často se vyskytující znak „a“ kódoval pěti bity a např. znak „˜“ třeba deseti. Jak takový kód zkonstruovat, aby bylo ušetřeného místa co nejvíce? Jak ušetřené místo vůbec měřit? To jsou velice zajímavé otázky, ale my na ně zde neodpovíme[1], neb budeme řešit kódování, které má jiné ambice.

Naším cílem bude nějaké důstojné popasování se s následující situací: Snažíme se poslat nějakou zprávu po síti. Řekněme, že jsme použili např. ASCII, a máme zprávu zapsanou nad binární abecedou $\{0, 1\}$. Jeden z bytů[2], které chceme poslat, odpovídá písmenu D: 01000100. Jak ale při přenosu po drátech[3] bývá, signál interferuje s okolím a jeden bit se nám pokazí: namísto 01000100 přijde adresátovi 010001**1**0. To může vést k nedorozumění[4], nepochopení textu apod., přesto adresát nemá šanci poznat, že se něco pokazilo, natož pak co přesně se pokazilo.

Kódování, které budeme v této kapitole zkoumat, bude mít ambici právě takovou situaci řešit. Budeme chtít zakódovat zprávu tak, aby měl příjemce šanci poznat, že nedorazila přesně ta zpráva, která byla odeslána a příp. dokonce i z pokažené zprávy tu původní rekonstruovat.

[1]Jen co dokončíte bakalářské studium, můžete si zapsat např. předmět MI-KOD: komprese dat, kde se dozvíte odpovědi nejen na tyto otázky.

[2]Aby bylo jasno: čteme „bajtů“.

[3]Nebo nedejbože po bezdrátech.

[4]Představte si situaci, že posílané D bylo z anglického slova „duck“!

4.1 Co si z této kapitoly odneseme

1. Řekneme si, co je abeceda, kódování, kód a vysvětlíme si, co přesně znamená, že nějaký kód umí objevovat či dokonce opravovat chyby.

2. Vysvětlíme si, co je lineární kód, že se vlastně jedná o podprostor vektorového prostoru $\mathbb{Z}_p^n$.

3. Díky Frobeniově větě a znalosti podprostorů si zavedeme dvě charakteristiky lineárních kódů: kontrolní a generující matici.

4. Ukážeme si, jak definovat dekódování tak, aby tam, kde je to možné, efektivně fungovalo tak, jak má.

5. Ukážeme si také, že většina práce při dekódování se dá odbýt násobením kontrolní maticí.

4.2 Základní pojmy a obecné vlastnosti samoopravných kódů

Tuto sekci začneme příklady, které by Vám měly usnadnit pochopení následně zavedených pojmů. Nejdříve si ale přeci jen dva pojmy zavedeme, a to úplně bez přípravy! Jedná se o pojmy abeceda a slovo, které už asi znáte, my jim zde ale poněkud rozšíříme platnost: abecedou (a písmeny) bude moci býti prakticky cokoli, neb abecedou bude moci být prakticky jakákoli konečná množina.

Definice 4.1. ***Abeceda*** *je jakákoli konečná neprázdná množina obsahující alespoň dva prvky*[5]*. Prvky abecedy nazýváme* ***písmena*** *(příp.* ***znaky****) a jakýkoli řetězec n písmen $a_1 a_2 \cdots a_n$, kde $n \in \mathbb{N}_0$, nazýváme* ***slovo*** *délky n. Je-li $n = 0$, mluvíme o* ***prázdném slově****.*

Množinu všech (konečných) slov nad abecedou[6] *$\mathcal{A}$ značíme $\mathcal{A}^*$ a množinu všech konečných neprázdných slov nad abecedou $\mathcal{A}$ značíme $\mathcal{A}^+$. Množinu všech slov nad abecedou $\mathcal{A}$, jejichž délka je n, značíme $\mathcal{A}^n$.*

Abecedou tedy zůstává i naše známá množina (českých) písmen {a,b,c,č,d,ď, …, z, ž}, neb se jedná o konečnou množinu. A každé slovo, které najdete ve slovníku, je stále slovem, neb se jedná o zřetězení konečně mnoha písmen. To platí pro abecedy všech jazyků[7] a dokonce i když vezmeme sjednocení všech abeced všech jazyků[8], dostaneme abecedu, neb se jedná o konečnou množinu. Trochu novinkou je, že pro nás je slovem (nad českou abecedou) i třeba „íáyjkwíáykjíá“ nebo „barbarkonanvenčípudla“, i když je ve slovníku nenajdeme.

[5] Obvykle se abeceda definuje jako úplně jakákoli konečná množina, tedy i jednoprvková. Pro nás by ale takové abecedy neměly moc smysl a jen bychom museli skoro všude opakovat předpoklad, že abeceda má alespoň dva prvky. Tak jsme tento předpoklad propašovali rovnou do definice.

[6] Divný výraz „slovo nad abecedou $\mathcal{A}$“ znamená „slovo, jehož písmena jsou z abecedy $\mathcal{A}$“. Se to takto prostě vžilo.

[7] Dokonce i v němčině jsou všechna slova konečná.

[8] Klidně i včetně klingonštiny.

V tomto textu se ale přirozeně zaměříme spíše na abecedy, které jsou blízké počítačům. Zejména se jedná o abecedu binární, tedy dvoupísmennou abecedu $\mathcal{A}_2 = \{0, 1\}$ s písmeny 0 a 1. Někdy se nám bude hodit považovat za abecedu i konečné množiny slov nad binární abecedou, např. „tříbitovou“ abecedu osmi slov

$$\mathcal{A}_2^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}.$$

Jedná se skutečně o abecedu, neb je to konečná množina, a např. 000 010 110 je třípísmenné slovo nad touto abecedou s písmeny 000, 010 a 110.

Takže už víme, co je abeceda, a tak se můžeme vrhnout ke slíbeným příkladům. Začneme jednoduchým tzv. **opakovacím kódem**, který spočívá prostě v tom, že kódované slovo několikrát zopakujeme.

Příklad 4.2 (3-opakovací kód)**.** *Uvažujme například tříbitová písmena z abecedy* $\mathcal{A}_2^3$ *uvedené výše. Každé písmeno budeme kódovat tak, že jej třikrát zopakujme: například budeme-li po síti chtít poslat tři bity* 010*, pošleme 9bitové slovo* 010010010*.*

Představme si nyní, že se během cesty po síti dva bity (řekněme 1. a 5.) pokazí a přepíšou se, namísto odeslaných devíti bitů 010010010 *přijme adresát bity* **1**100**0**0010*. Pokud adresát ví, že používáme opakovací kód, bude mu hned jasné, že se stala někde chyba (tomuto budeme říkat, že kód objevuje chyby). Když se nad tím zamyslíte*[9]*, zjistíte, že když se stanou dvě chyby kdekoli, tak to adresát vždy pozná. Ovšem kdybychom měli smůlu, a chyby se staly tři na 1., 4. a 7. bitu, adresát by dostal slovo* **1**10**1**10**1**10 *a neměl by důvod si myslet, že je něco špatně. Pochopitelně by si domyslel, že odeslané slovo (přesněji písmeno) pravděpodobně bylo* 110*. Abychom postihli i tuto vlastnost, budeme říkat, že tento kód objevuje 1 chybu, 2 chyby, ale 3 chyby již nikoli!*

Samozřejmě kdyby se chyby staly na jiných místech, třeba 1., 5. a 9. bitu, tak to poznáme i tak. Abychom ale mohli říci, že kód objevuje 3 chyby, musí je umět odhalit, ať se stanou kdekoli!

Na vysvětlenou je třeba také dodat, že když se stanou čtyři chyby, např. na 1., 4. 7. a 8. bitu, dostane adresát slovo **1**10**1**10**1**0**0** *a řekne si: „Aha! Tady to nesedí, stala se jedna chyba na 8. bitu, původně tam byla* 1*“ a ještě si bude myslet jak je chytrý. Takové situace jsou možné a žádný kód není odolný vůči libovolnému počtu chyb*[10]*, obecně ale v teorii samoopravovacích kódů pracujeme s předpokladem, že* ***výskyt méně chyb je pravděpodobnější než výskyt více chyb****. Tento*[11] *předpoklad ospravedlňuje adresáta, který slovo* **1**10**1**10**1**0**0** *„přečte“ jako odeslané* 110*, protože předpokládá, že je pravděpodobnější, že nastala jedna chyba ve slově* 110110110 *než že nastaly čtyři chyby ve slově* 010010010*.*

Náš opakovací kód tedy objevuje až dvě chyby, ale má ještě jednu vlastnost, kterou jsme již naznačili: Když nastane právě jedna chyba, umíme z přijatého slova dokonce zjistit, kde nastala. Např. dostane-li adresát slovo 010010**1**10*, může se zcela oprávněně domnívat, že původní odeslané slovo bylo ve skutečnosti* 010010010 *a že nastala*

[9] Zamýšlení obecně doporučujeme!

[10] Když si např. připustíme, že se stane v devíti bitovém slově až devět chyb, je možné cokoli, kód nekód.

[11] Imho rozumný.

chyba v 7. bitu. Když se stanou dvě chyby, tak už se může stát, že oprava povede k chybnému závěru. Např. slovo **1**10010**1**10 *už je rozumnější opravit na* 110110110 *než na skutečně odeslané* 010010010*. Kdyby se ale staly chyby jinde, např.* 0**0**0010**1**10*, bude rozumnější slovo opravit správně na* 010*, protože každé jiné slovo z našeho opakovacího kódu je od* 0**0**0010**1**10 *„vzdáleno" o více než dvě chyby: např. kdyby odesílané slovo bylo* 000000000*, musely by nastat chyby tři, a to považujeme za méně pravděpodobné.*

To, že nějaký kód dovoluje chyby nejen objevit[12] *ale dokonce i opravit*[13]*, budeme pojmenovávat jako opravování chyb. Konkrétně náš opakovací kód opravuje 1 chybu, ale více ne, neboť 2 chyby už opravit umět nemusí.*

Kdybychom předchozí příklad zobecnili, mohli bychom říci, že když odesílané tři bity nezopakujeme třikrát, ale $n$krát, dostaneme kód, který objevuje $n-1$ chyb a opravuje $\lfloor\frac{n-1}{2}\rfloor$ chyb[14]. Takže můžeme zkonstruovat kód, který objevuje a opravuje tolik chyb, kolik si řekneme. Nabízí se ale přirozená otázka, jestli by to nešlo udělat šetrněji, tedy např. chci-li objevovat jednu chybu, musím opravdu zprávu dvakrát prodloužit a místo např. 99 bitů jich posílat 198? Ukážeme si kód, který pro objevování 1 chyby potřebuje dokonce jediný bit navíc. Je to takzvaný **paritní kód**.

Příklad 4.3 (Paritní kód)**.** *Obecně paritní kód funguje takto: Mějme n bitové slovo $b_1 b_2 \cdots b_n \in \mathcal{A}_2^n$. Toto slovo zakódujeme tak, že k němu přidáme jeden bit b_{n+1} tak, aby počet jedniček ve výsledném slově $b_1 b_2 \cdots b_n b_{n+1}$ byl sudý.*

Např. pro $n = 3$ dostáváme „kódovací tabulku"

původní slovo	*000*	*001*	*010*	*011*	*100*	*101*	*110*	*111*
zakódované slovo	*0000*	*0011*	*0101*	*0110*	*1001*	*1010*	*1100*	*1111*

Všimněte si, že ve druhém řádku je vždy sudý počet jedniček.

Teď si představme, že v jednom ze zakódovaných slov uděláme chybu, tj. přepíšeme 0 *na* 1 *nebo naopak. Výsledné slovo pak bude obsahovat o jedno písmeno* 1 *více nebo méně než původní, tedy jedniček bude lichý počet. Tak poznáme, že se chyba stala, neb bezchybná slova mají sudý počet jedniček, a paritní kód tedy skutečně objevuje 1 chybu.*

Snadno si rozmyslíte, že paritní kód neobjevuje více chyb. Dokonce platí, že když se stanou právě dvě chyby úplně kdekoli, tak nepoznáme vůbec nic, neb vždy dostaneme jiné validní kódové slovo se sudým počtem jedniček.

O opravování chyb také nemůže být řeč: z konstrukce kódu je jasné, že sice objevuje 1 chybu, ale nemáme šanci poznat, kde tato chyba nastala (mohla nastat kdekoli).

V předchozích dvou příkladech jsme se oháněli několika pojmy, které jsme zatím řádně nezavedli[15]. Předně jsme si zatím neřekli, co je to vlastně to kódování. Už v

[12] „Ha! Něco je špatně!"

[13] „Ha! Něco je špatně a navíc vím kde a co!"

[14] Toto si prosím rozmyslete a pochopte alespoň na úrovni „když n je 5, tak chápu, proč kód objevuje 4 chyby a opravuje jen 2".

[15] Definice příkladem je sice pedagogicky vhodná, ale z pohledu matematiky by byla hanba, u takové definice zůstat!

úvodu jsme si řekli, že kódování je „přepis jednoho řetězce znaků (neboli slova resp. písmena) z nějaké abecedy na jiný řetězec znaků z jiné či stejné abecedy.“ Jelikož ten přepis je jednoznačný, tj. jedno slovo vždy přepíšeme stejně, jedná se vlastně o zobrazení. A přesně jako zobrazení kódování definujeme:

Definice 4.4 (kódování, kód)**.** *Mějme dvě abecedy $\mathcal{A}$ a $\mathcal{B}$. Každé zobrazení $\kappa : \mathcal{A} \to \mathcal{B}^+$ nazýváme **kódováním**[16]. Obor hodnot tohoto zobrazení $H_\kappa \subseteq \mathcal{B}^+$ nazýváme **kód** a libovolné slovo z H_κ nazýváme **kódové slovo**.*

Zobrazení přirozeně rozšiřujeme na slova z $\mathcal{A}^+$ takto: buď $u = u_1 u_2 \cdots u_n \in \mathcal{A}^n$ slovo délky n s písmeny $u_i \in \mathcal{A}$. Potom

$$\kappa(u) = \kappa(u_1)\kappa(u_2)\cdots\kappa(u_n).$$

Pro 3-opakovací kód z příkladu 4.2 platí toto:

Příklad 4.5 (3-opakovací kód, pokračování)**.** *Kdybychom měli zavést 3-opakovací kód znovu s využitím značení z předchozí definice, bylo by to takto: Za abecedu $\mathcal{A}$ bychom vzali množinu 3bitových písmen*[17]

$$\mathcal{A}_2^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$$

a za abecedu $\mathcal{B}$ pak binární abecedu[18]*. Zobrazení, které definuje 3-opakovací kód obecně funguje tak, že písmenu u (tj. 3bitovému slovu z abecedy $\mathcal{A}_2^3$) přiřadí slovo $\kappa(u) = uuu$. Pro naši volbu abecedy $\mathcal{A}$ je zobrazení κ popsáno tabulkou*

u	*000*	*001*	*010*	*011*
$\kappa(u)$	*000000000*	*001001001*	*010010010*	*011011011*
u	*100*	*101*	*110*	*111*
$\kappa(u)$	*100100100*	*101101101*	*110110110*	*111111111*

Kódem je pak obor hodnot tohoto zobrazení, tedy osm slov z druhého řádku tabulky. Tato slova dle definice nazýváme kódovými slovy.

Kdybychom tedy tento kód chtěli použít na slovo 001000110, pak jej zakódujeme do tří kódových slov

$$\kappa(001000110) = \kappa(001)\kappa(000)\kappa(110) = 001001001\,000000000\,110110110.$$

Aby to bylo kompletní, uvedeme i jak formálně zavést paritní kód:

Příklad 4.6 (Paritní kód)**.** *Jako vstupní abecedu $\mathcal{A}$ můžeme vzít množinu všech binárních slov délky $n \in \mathbb{N}$, tedy množinu $\mathcal{A}_2^n$ obsahující 2^n slov. Jako koncovou abecedu $\mathcal{B}$ pak bereme binární abecedu $\mathcal{A}_2$ a obor hodnot je pak podmnožinou binárních slov délky $n+1$. Abychom formálně popsali, jak vypadá zobrazení κ pro paritní kód, uvědomíme si jednu věc, na které bude vlastně vidět důvod, proč o kódech mluvíme v tomto textu o lineární algebře: Jako abecedu můžeme dle definice chápat jakoukoli*

[16] To divné písmenko κ je řecká kappa.

[17] Že říkáme 3písmenným slovům písmena? Je to konečná alespoň dvouprvková množina? Je! Tak kde je problém?! Abeceda je každá konečná alespoň dvouprvková množina!

[18] Kódová slova mají všechny délku 9, binárních slov délky 9 je celkem $2^9 = 512$. Z pochopitelných důvodů je zde nebudeme vypisovat.

konečnou množinu, tedy i konečná tělesa! Binární abeceda $\mathcal{A}_2$ je tak vlastně totožná s konečným tělesem $\mathbb{Z}_2$ a slova délky n jsou vlastně vektory[19] *z vektorového prostoru $\mathbb{Z}_2^n$. Když tedy přistoupíme*[20] *na to, že slovo $b_1b_2\cdots b_n$ je vlastně vektor $(b_1, b_2, \ldots, b_n)$ z vektorového prostoru $\mathbb{Z}_2^n$. Můžeme paritní kódování κ zapsat takto:*

$$\kappa(b_1b_2\cdots b_n) = b_1b_2\cdots b_nb_{n+1}, \quad \textit{kde } b_{n+1} = b_1 + b_2 + \cdots + b_n.$$

Při sčítání písmen/čísel z tělesa používáme sčítání z tělesa $\mathbb{Z}_2$, tedy sčítání modulo 2. Např. pro $n = 3$ a slovo $b_1b_2b_3 = 110$ pak dostáváme $b_4 = 1 + 1 + 0 = 0$ a tedy $\kappa(110) = 1100$.

Obor hodnot kódování κ, tedy paritní kód, pak můžeme popsat jako podmnožinu slov/vektorů z $\mathbb{Z}_2^{n+1}$, které vyhovují rovnici

$$b_1 + b_2 + \cdots + b_{n+1} = 0.$$

Tato rovnice skutečně platí pouze, pokud mezi písmeny b_1 až b_{n+1} najdeme sudý počet jedniček.

Takže už jsme si vyjasnili, co je to to kódování a kód. Zbývá nám si vyjasnit, co je to přesně to objevování a opravování chyb. Začneme tím, že si přesně řekneme, co považujeme za chybu, což je zřejmě dosti nerigorózní pojem. Chyb může vzniknout ve slově mnoho, jedno písmeno se přepíše na jiné, dvě písmena se prohodí, část slova se ztratí, či se nám do slova vloudí nějaká písmena navíc[21]. Teorie kódování je už poměrně stará disciplína a navíc stále živá, takže se stále konstruují nové kódy pro nové situace, kdy jsou různé druhy chyb různě pravděpodobné. My v tomto textu budeme uvažovat jediný druh chyby:

> **Za chybu považujeme pouze přepis jednoho písmena na jiné písmeno dané abecedy. Jiné druhy chyb v tomto textu neuvažujeme.**

V příkladu 4.2 jsme si řekli, že 3-opakovací kód objevuje 2 chyby, ale už ne tři. Důvod byl ten, že když uděláme tři chyby na „vhodných“ bitech, dostaneme z jednoho kódového slova jiné kódové slovo a adresát pak neví, že se stalo něco špatného. Konkrétně jsme si to ukázali na příkladu kódového slova 010010010: Když se stanou chyby v 1., 4. a 7. bitu, dostaneme slovo 110110110, což je také kódové slovo a o žádné chybě tak nemáme tušení. Když se ale stanou dvě chyby, tak už se nám nemůže stát, že bychom z jednoho kódového slova získali jiné. Jak tuto vlastnost zachytit formálně a přesně? Využijeme k tomu definici vzdálenosti dvou slov, která by měla mít následující vlastnost: Vzdálenost dvou (stejně dlouhých) slov je rovna k, jestliže z jednoho slova můžeme vyrobit to druhé tak, že uděláme k chyb, tj. přepisů jednoho písmene na druhé, a toto k je nejmenší možné s touto vlastností (tj. méně chyb nám ke změně jednoho slova na druhé nestačí). Taková vzdálenost je ale v informatice celkem známá a říká se jí Hammingova vzdálenost slov:

[19] Slova jsou skutečně vlastně uspořádané $n$tice písmen, no a když jsou písmeny 0 a 1, tak uspořádanou $n$tici písmen můžeme přirozeně chápat i jako uspořádanou $n$tici čísel z tělesa, tedy jako vektor!

[20] Kdo na to nepřistoupí, bude zejména v příští kapitole trpět.

[21] Pokud děláte překlepy, tak máte celkem dobrou představu, co se může stát.

Definice 4.7. *Pro dvě slova $u = u_1 u_2 \cdots u_n$ a $v = v_1 v_2 \cdots v_n$ stejné délky n a nad stejnou abecedou definujeme **Hammingovu vzdálenost** jako*

$$d(u, v) = \text{ počet indexů } i \in \hat{n} \text{ takových, že } u_i \neq v_i.$$

Pro příklad dvou slov výše tedy platí

$$d(010010010, 110110110) = 3,$$

neb se liší na třech místech (s indexy 1, 4, 7).

Pro paritní kód z příkladu 4.6 platí, že každé dvě kódová slova mají Hammingovu vzdálenost alespoň dva[22]. Nemůže se tedy stát, že uděláme jednu chybu a z jednoho kódového slova vyrobíme jiné, k tomu je potřeba vždy alespoň dvou chyb.

Představme si, že by nějaký neuvážlivec vymyslel kód s kódovými slovy 0000, 0010, 1100 a 1111. Kolik tento kód objevuje chyb? Kdybychom chtěli poslat adresátovi kódové slovo 0000 a měli smůlu, mohla by se stát chyba ve třetím bitu. Adresát by přijal slovo 0010, což je taky kódové slovo, takže by neměl důvod si myslet, že nějaká chyba nastala. Tento kód tedy neobjevuje ani jednu chybu! A proč tomu tak je? Protože obsahuje dvě kódová slova, jejichž Hammingova vzdálenost je jedna. A právě toto číslo, které udává vzdálenost dvou *nejbližších* kódových slov, je velmi důležitou charakteristikou kódu[23]. Zavedeme si jej tedy v definici spolu s příslušným značením.

Definice 4.8. *Pro kód K definujeme a značíme **minimální vzdálenost kódu** jako*

$$\mu(K) = \min\{d(u, v) \mid u, v \in K, u \neq v\}.$$

Minimální vzdálenost paritního kódu je tedy 2. Pro n-opakovací kód (každé kódované slovo $n$krát opakuje), který si označíme K^n, je pak minimální vzdálenost rovna n, tedy $\mu(K^n) = n$.

V předchozím textu jsme si (snad) vše dostatečně vysvětlili, takže teď již můžeme zavést formální definici toho, že kód objevuje chyby. Tato definice zachycuje myšlenku, že kód objevuje t chyb, jestliže se z žádného kódového slova nedostanu na jiné kódové slovo tím, že v něm přepíšu t písmen.

Definice 4.9. *Řekneme, že kód K **objevuje t chyb**, jestliže $\mu(K) > t$.*

Paritní kód tedy objevuje jednu chybu, ale už ne dvě chyby. Opakovací kód K^n má minimální vzdálenost n, a tedy objevuje t chyb, kde $t = 1, 2, \ldots, n-1$. Často je pro nás nejzajímavější nejvyšší možná hodnota t; abychom toto zdůraznili, budeme například říkat, že kód K^n objevuje *nejvýše* $n-1$ chyb.

U opravování chyb je to trochu složitější: Nestačí nám detekovat to, že přijaté slovo není jedno z kódových slov, ale navíc musíme být schopni určit, které kódové slovo bylo odesláno. Toto určování odeslaného kódového slova se týká procesu dekódování, kterému se budeme podrobně věnovat až v poslední části této kapitoly, teď

[22] Zkuste si rozmyslet, že Hammingova vzdálenost dvou kódových slov paritního kódů je vždy sudá.

[23] „Každý řetěz je silný jen tak, jak je silný jeho nejslabší článek.“ *Arthur Conan Doyle, J. Watson – Údolí strachu*

nám bude stačit základní pochopení. Dekódování bude probíhat v zásadě takto[24]: Předpokládejme, že používáme kód K a přijmeme slovo u (toto slovo může a nemusí obsahovat chyby).

1. Pokud je u kódové slovo, tj. $u \in K$, dekódujeme jej jako u, neb nemáme důvod se domnívat, že při jeho přenosu došlo k nějakým chybám.
2. Pokud není u kódové, tj. $u \notin K$, najdeme všechna kódová slova, která jsou u nejblíže.
3. Pokud je toto nejbližší slovo jediné, označme jej jako v, budeme předpokládat, že to je slovo, které bylo původně odesláno a u dekódujeme jako v.
4. Pokud je těchto nejbližších slov více, tak buď nahlásíme, že nevíme, nebo si vybereme dle nějakého klíče, nebo třeba i náhodně.

Příklad 4.10 (Opakovací kód K^4)**.** *Uveďme si příklad na opakovacím kódu K^4, který spočívá v 4násobném opakování 3bitového slova. Předpokládejme, že přijaté slovo je* 011011011011*. Toto slovo je kódové, takže jej dekódujeme jako* 011011011011 *a předpokládáme tak, že skutečné odeslané slovo bylo* 011*.*

Pokud bychom přijali slovo 011011011001*, které není kódové, pokusíme se najít všechna nejbližší kódová slova. Jediné kódové slovo* 011011011011 *je od našeho přijatého slova ve vzdálenosti* 1*. Všechna ostatní kódová slova mají vzdálenost vyšší*[25]*. Slovo* 011011011001 *tedy dekódujeme jako* 011011011011*.*

Pokud by námi přijaté slovo bylo 001011011001*, tak najdeme dvě nejbližší kódová slova: Slova* 011011011011 *a* 001001001001 *mají od našeho slova* 001011011001 *obě Hammingovu vzdálenost* 2*. Při přijetí slova* 001011011001 *tedy buď nahlásíme, že se dekódování nezdařilo, nebo si z těchto dvou slov náhodně vybereme*[26]*.*

V definici opravování chyb se tedy budeme snažit postihnout počet chyb, při kterých je výše popsaná dekódovací procedura vždy schopná najít správné kódové slovo. V našem příkladu to byla pouze jedna chyba, neb už u dvou chyb jsme mohli dostat dvě stejně vzdálená kódová slova. Důvod je ten, že minimální vzdálenost kódu K^4 je čtyři, proto se již při dvou chybách můžeme dostat „přesně mezi“ dvě kódová slova a jednoznačné dekódování již není možná. Kdybychom chtěli opravovat dvě chyby, museli bychom použít kód K^5.

Definice 4.11. *Řekneme, že kód K* ***opravuje*** *t* ***chyb****, jestliže $\mu(K) > 2t$.*

Kód, který by měl opravovat 1 chybu, nesmí mít minimální vzdálenost menší než 3, pro opravu dvou chyb už potřebujeme minimální vzdálenost 5 atd. Kód, jehož minimální vzdálenost je $n > 2$, opravuje nejvýše $\lfloor \frac{n-1}{2} \rfloor$ chyb.

[24] Na konkrétních příkladech už jsme to vlastně předvedli výše, aniž bychom tomu říkali dekódování.

[25] Zkuste si rozmyslet, že vzdálenost od libovolného kódového slova je rovna $1 + 4k$ pro nějaké $k \in \mathbb{N}_0$.

[26] Jsou situace, kdy je lepší nějaké dekódování provést, než proces přijímání zpráv zastavit či nějak komplikovat. Např. čteme-li data z CD při hraní hudby, není nejlepší strategie hudbu zastavit kdykoli se čtení takto pokazí. Pro neznalé: CD je takové kolečko, na které se ukládala data na začátku tohoto tisíciletí. Vy se s touto starožitnou technologií nejspíše setkáte při odevzdávání Vaší bakalářské práce.

Informační a kontrolní znaky, systematický kód

Nyní už umíme určit, kolik chyb daný kód objevuje a opravuje. To ale není jediný atribut kódu, který by nám říkal, jak je kód dobrý. Například kódujeme-li paritním kódem nebo opakovacím kódem K^2 tříbitová binární slova, dostáváme dva různé kódy s minimální vzdáleností dva, které každý objevují jednu a neopravují žádnou chybu. Kódová slova paritního kódu budou čtyřbitová, neboť ke zvětšení minimální vzdálenosti na dva, nám stačil jeden bit. Budeme říkat, že tento paritní kód obsahuje 3 bity (resp. písmena či znaky), které nesou informaci, a jeden jediný, který je tzv. kontrolní. Naopak opakovací kód potřeboval ke zvětšení minimální vzdálenosti na dva celé tři bity: z celkových 6 bitů kódového slova tak pouze 3 nesou informaci o odesílaném slově a zbylé 3 jsou kontrolní. Z jistého pohledu je tedy paritní kód třikrát úspornější, než uvedený kód opakovací.

Abychom si tyto pojmy definovali obecně, budeme muset předpokládat vlastnost kódu, se kterou jsme v našich dosavadních příkladech vždy jen tak mimochodem počítali, tedy že kódová slova jsou všechna stejné délky. To lze formálně zapsat tak, že kódování κ z definice 4.4 je zobrazení do množiny $\mathbb{B}^\ell$ pro nějaké $\ell \in \mathbb{N}$. Např. výše uvedený paritní kód je zobrazení z $\mathbb{Z}_2^3$ do $\mathbb{Z}_2^4$ a opakovací kód ze $\mathbb{Z}_2^3$ do $\mathbb{Z}_2^6$.

Definice kódování tuto vlastnost ale nevyžaduje. Např. zobrazení z množiny $\{a, b, c\}$ do slov nad binární abecedou definované jako $\kappa(a) = 1, \kappa(b) = 01, \kappa(c) = 001$ je korektně definované kódování, ale těžko budeme určovat, kolik přesně bitů nese informaci a kolik nikoli[27].

Dva výše uvedené příklady by mohli vést k domněnce, že jako informační počet znaků vezmeme prostě počet znaků, které obsahovalo kódované slovo (např. 001), a počet kontrolních znaků pak bude určen tím, kolik znaků jsme museli přidat, abychom z tohoto slova vyrobili slovo kódové (0011 pro paritní kód resp. 001001 pro opakovací). To by byla nešikovná definice, protože kódování nemusí být vždy tak přímočaré. V definici 4.4 mohou být vstupní abeceda $\mathcal{A}$ a výstupní abeceda $\mathcal{B}$ obecně různé a tak by nám podobné počty mohly zkolabovat. Uvažujme například kódování $\kappa : \{a, b, c, d\} \to \mathbb{Z}_2^3$ z čtyřpísmenné abecedy do čtyřbitových řetězců zadané následovně:

$$\kappa(a) = 000, \kappa(b) = 011, \kappa(c) = 101, \kappa(d) = 110.$$

S trochou fantazie lze říci, že se jedná vlastně o paritní kód, který jsme získali tak, že jsme přepsali čtyři písmena a, b, c, d do dvou bitů: $00, 01, 10, 11$, a následně přidali jeden bit tak, abychom získali paritní kód. I zde můžeme intuitivně říci, že dva bity nesou informaci a třetí je tam pro kontrolu, abychom mohli objevit jednu chybu. Kvůli těmto nuancím definujeme informační a kontrolní znaky následovně.

Definice 4.12. *Řekneme, že kód $K \subseteq \mathcal{B}^n$ (tj. předpokládáme, že kódová slova mají stejnou délku!) má k* ***informačních znaků*** *a $n - k$* ***kontrolních znaků****, jestliže existuje bijekce $\varphi : \mathcal{B}^k \to K$.*

[27] Ne že by to nešlo udělat, ale vyžadovalo by to trochu sofistikovanější metody, kterými si jednoduchou lineární algebru nebudeme kazit (viz např. pojem entropie)).

Když mezi dvěma konečnými množinami existuje bijekce, mají tyto dvě množiny nutně stejně prvků[28]. Předchozí definici bychom tedy mohli ekvivalentně přepsat tak, že kód $K \subset \mathcal{B}^n$ má k informačních znaků, jestliže obsahuje tolik kódových slov, kolik slov obsahuje množina $\mathcal{B}^k$. Např. pro binární abecedu $\mathcal{B} = \mathbb{Z}_2$ dostáváme následující: kód $K \subset \mathbb{Z}_2^n$ má k informačních znaků, právě když obsahuje právě 2^k kódových slov.

Paritní a opakovací kód, tak jak jsme si je zadefinovali, mají jednu pěknou vlastnost: je velmi jednoduché v nich identifikovat ty znaky, které nesou informaci[29] (jsou vždy na začátku) a ty, které jsou kontrolní (jsou vždy až za těmi informačními). To je zejména z pohledu implementace velmi výhodné[30]. Chceme-li například kódovat tříbitová slova $000, 001, \dots, 111$ paritním kódem, tak slovo přečteme, dopočítáme čtvrtý bit a ten za přečtené slovo prostě připojíme. Podobně pro opakovací kód, tam budeme pouze připojovat více bitů.

Tuto vlastnost nemá tzv. **koktavý kód**, což je vlastně jinak pojatý opakovací kód. Například tříbitová slova by 2-koktavý kód zakódoval následovně:

původní slovo	000	001	010	011	100	101	110	111
zakódované slovo	000000	000011	001100	001111	110000	110011	111100	111111

Na rozdíl od opakovacího kódu koktavý kód neopakuje celá slova, ale jednotlivá písmena. Uvedený koktavý kód (opakující písmena dvakrát) má stejně jako opakovací kód (opakující slovo dvakrát) minimální vzdálenost dva. Objevuje tedy 1 chybu a neopravuje žádnou. Nemá ale tu vlastnost, kterou popisujeme v předchozím odstavci: kódujeme-li např. slovo 010, nestačí nám přidat tři bity za toto slovo, ale musíme vytvořit slovo úplně nové. To, jestli tuto vlastnost má nebo nemá, poznáme snadno podle úvodních k znaků, kde k je počet informačních znaků dle definice 4.12. Přečteme-li u našich tří kódů se třemi informačními znaky (tj. $k = 3$) první tři bity všech kódových slov, zjistíme, že pro paritní a opakovací kód jsou tyto tři bity pro různá kódová slova odlišná, kdežto pro koktavý kód máme např. dvě kódová slova, začínající třemi bity 001.

Definice 4.13. *Mějme kód $K \subset \mathcal{B}^n$ s k informačními a $n - k$ kontrolními znaky. Lze-li bijekci φ z definice 4.12 zvolit tak, že pro každé $u \in \mathcal{B}^k$ existuje $v \in \mathcal{B}^{n-k}$ takové, že*

$$\varphi(u) = uv \in K,$$

*říkáme, že K je **systematický kód**.*

Obecně lze říci, že dobrý kód poznáme z poměru minimální vzdálenosti, která určuje, kolik chyb kód objevuje a opravuje, a počtu kontrolních znaků, který určuje, jak moc nám kód bude zvětšovat odesílané zprávy. Následující věta nám říká ve vší obecnosti, v jakou nejvyšší minimální vzdálenost můžeme doufat, když používáme systematické kódy.

[28] Nejen nutně, ale i „postačujícně“: existence bijekce mezi dvěma konečnými množinami je ekvivalentní s tím, že mají stejně prvků. U nekonečných množin mluvíme o stejných mohutnostech.

[29] Pojem „nést informaci“ jsme si nedefinovali, ale věříme, že laskavý čtenář intuitivně tuší, co tím myslíme.

[30] Kódování se odehrává obvykle na nejnižších vrstvách komunikace a je pro něj klíčové, aby bylo rychlé a dalo se provádět prakticky okamžitě bez potřeby nějakých významnějších nebo sofistikovanějších výpočetních zdrojů. Viz také předmět BI-SAP: struktura a architektura počítačů.

Věta 4.14. *Je-li $K \subseteq \mathcal{B}^n$ systematický kód s k informačními znaky, platí pro jeho minimální vzdálenost*

$$\mu(K) \leq n - k + 1.$$

Důkaz. Důvod, proč minimální vzdálenost nemůže překonat počet kontrolních znaků o více než jedna, plyne z následující vlastnosti systematického kódu: Máme-li kód s k informačními znaky, pak množina slov délky k, která tvoří prefixy[31] všech kódových slov, tvoří množinu všech slov délky k, tedy $\mathcal{B}^k$. Skutečně tomu tak je, stačí si uvědomit, že zobrazení φ z definice systematického kódu je bijekce mezi množinou kódových slov a množinou $\mathcal{B}^k$, která navíc funguje tak, že obraz každého slova z $\mathcal{B}^k$ je pouze nějakým jeho prodloužením.

Vezměme si nyní nějaké slovo v z $\mathcal{B}^{k-1}$. V kódu díky výše uvedené vlastnosti (a díky tomu, že v abecedě jsou alespoň dvě písmena) existují alespoň dvě kódová slova, která začínají slovem v (neboli v je jejich prefix). Tato slova délky n mají shodných alespoň prvních $k-1$ znaků, a tedy jejich Hammingova vzdálenost je nejvýše $n-(k-1)$. Z toho již jednoduše plyne, že minimální vzdálenost kódu také nemůže být větší než toto číslo.

□

Pro paritní kód, který má jediný kontrolní znak, je hranice „počet kontrolních znaků + 1" tedy dosaženo[32], neb jeho minimální vzdálenost je dva. U opakovacích kódů už hranice dosažená není, např. pro K^3 pro tříbitová slova je počet kontrolních znaků 6, ale minimální vzdálenost je tři.

4.3 Lineární kódy

Spojení teorie samoopravovacích kódů s lineární algebrou spočívá v již dříve uvedené myšlence, že konečné těleso $\mathbb{Z}_p$ lze zároveň chápat jako abecedu a že vektory ze $\mathbb{Z}_p^n$ lze chápat jako slova délky n. Ve zbytku této kapitoly tento dvojí pohled dotáhneme tak daleko, že rozdíl mezi slovem a vektorem úplně smažeme. Budeme tedy slova sčítat (po složkách modulo prvočíslo p) a násobit číslem z tělesa $\mathbb{Z}_p$. Ze slov budeme tvořit matice a budeme je maticemi násobit: např. výsledkem násobení slova 00110 ze $\mathbb{Z}_2^5$ maticí

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

(myslíme násobení maticí zleva a tedy slovo bereme jako sloupcové) bude slovo 110, neboť platí

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}.$$

[31]Latina! Myslíme tím v tomto případě prvních k znaků kódového slova, je-li např. $k = 3$ a 00110101 kódové slovo, je jeho prefix délky k slovo 001.

[32]Takový kód se nazývá perfektní.

Když se tedy smíříme s tímto ztotožněním slova a vektoru, můžeme říci[33], že dle definice kódu je každá neprázdná podmnožina vektorového prostoru $\mathbb{Z}_p^n$ kódem. Ovšem ne každou takovou podmnožinu nazveme kódem lineárním: aby se jednalo o lineární kód, bude muset podmnožina $\mathbb{Z}_p^n$ tvořit podprostor.

Tím, že budeme požadovat, aby byl kód podprostorem, můžeme použít mnoho užitečných věcí, které jsme si o podprostorech řekli dříve. Klíčové budou hlavně dvě věci:

1. Každý netriviální podprostor VP $\mathbb{Z}_p^n$ má bázi.
2. Každý podprostor lze zapsat jako množinu řešení homogenní soustavy rovnic[34].

Definice 4.15. *Podmnožinu K vektorového prostoru $\mathbb{Z}_p^n$ nazveme* ***lineární*** (n,k)***-kód****, jestliže je K podprostor dimenze k.*

Nechť $k \in \{1,2,\dots,n-1\}$[35]. Matici $G_K \in \mathbb{Z}_p^{k,n}$, jejíž řádky tvoří bázi K, nazýváme ***generující maticí*** *K, matici $H_K \in \mathbb{Z}_p^{n-k,n}$ takovou, že K je množina řešení soustavy $H_K\mathbb{x} = \theta$, nazýváme* ***kontrolní maticí*** *K.*

Máme-li (n,k)-kód K, je dle definice jeho dimenze (jakožto podprostoru $\mathbb{Z}_p^n$) rovna k. Z toho lze vyvodit mnoho věcí:

1. Každá báze K obsahuje k vektorů (tj. slov) a jelikož každé kódové slovo má n písmen, má generující matice n sloupců a k řádků.
2. Pro kontrolní matici H_K platí, že K je množina řešení rovnice $H_K\mathbb{x} = \theta$. Dle Frobeniovy věty[36] je $k = \dim K = n - \mathrm{h}(H_K)$. Z toho plyne, že hodnost kontrolní matice H_K je rovna $n-k$ a tedy tato matice má alespoň $n-k$ řádků (určitě má n sloupců). V definici požadujeme, aby měla právě $n-k$ řádků, což vlastně znamená, že soubor vektorů obsahující její řádky musí být lineárně nezávislý.
3. Jelikož řádky generující matice G_K jsou vlastně kódová slova splňující rovnici $H_K\mathbb{x} = \theta$, platí[37] toto:
$$H_K G_K^T = \Theta \in \mathbb{Z}_p^{n-k,k} \quad \text{a tedy i} \quad G_K H_K^T = \Theta \in \mathbb{Z}_p^{k,n-k},$$
kde druhá rovnost plyne z první: stačí součin matic v první rovnosti transponovat.
4. Jelikož těleso/abeceda $\mathbb{Z}_p$ obsahuje p písmen, obsahuje každý podprostor K dimenze k právě p^k vektorů/slov. Existuje tedy bijekce mezi podprostorem

---

[33] A budeme mít pravdu.

[34] Skutečně, viz větu 3.41, která říká, že každou varietu lze zapsat jako řešení soustavy rovnic $\mathbb{A}\mathbb{x} = \mathbb{b}$. Podprostor je taky varieta, za jejíž vektor posunutí lze vzít nulový vektor. Z toho nutně plyne, že $\mathbb{b} = \theta$.

[35] Lineární (n,k)-kódy pro $k \in \{1,n\}$ jsou pro nás nezajímavé a nebudeme se jimi zabývat. Laskavý čtenář se jistě sám zamyslí, proč tomu tak je.

[36] Použijeme-li značení z Frobeniovy věty 3.24, je K vlastně množina řešení homogenní soustavy značená S_0.

[37] Rozmyslete si, jak funguje maticové násobení!

K a množinou $\mathbb{Z}_p^k$. To dle definice 4.12 znamená, že každý lineární (n,k)-kód obsahuje k informačních a $n-k$ kontrolních znaků. To je tak význačné zjištění, že si jej dáme do věty.

Věta 4.16. *Lineární (n,k)-kód má k informačních a $n-k$ kontrolních znaků.*

Důkaz. Tuto skutečnost můžeme dokázat i konstruktivně, takovou bijekci mezi K a $\mathbb{Z}_p^k$ nalezneme. Mějme libovolné slovo $a = a_1a_2\cdots a_k \in \mathbb{Z}_p^k$. Definujeme zobrazení $\varphi : \mathbb{Z}_p^k \to \mathbb{Z}_p^n$ předpisem

$$\varphi(a) := (a_1 \ a_2 \ \cdots \ a_k) \cdot G_K\,,$$

které každému slovu délky k přiřadí slovo délky n, a navíc ne ledajaké! Rozebere-li si laskavý čtenář, co přesně se děje při násobení „řádek krát matice“, zjistí, že $\varphi(a)$ je rovno lineární kombinaci řádků matice G_K. Tedy pro každé $a \in \mathbb{Z}_p^k$ platí $\varphi(a) \in K$. Současně je toto přiřazení vzájemně jednoznačné (neboli bijekce), protože obraz $\varphi(a)$ je vždy kódovým slovem s tou vlastností, že $(a_1, a_2, \ldots, a_k)$ jsou jeho **souřadnice** vůči bázi K, která je tvořena řádky generující matice G_K[38]. □

Už jsme si toho o lineárních kódech řekli docela hodně, ale ještě jsme si žádný neukázali. Tedy přesněji řečeno jsme si ještě o žádném kódu explicitně neřekli, že je lineární (ve skutečnosti jsme si ukazovali převážně lineární kódy).

Příklad 4.17 (Paritní kód je lineární)**.** *Zavzpomínejme si nyní na paritní kód z příkladu 4.6. Předpokládejme, že kódová slova mají délku n, jsou to tedy vlastně slova/vektory z vektorového prostoru $\mathbb{Z}_p^n$. Je množina kódových slov paritního kódu podprostorem? Už v příkladu 4.6 jsme si ukázali, že $b_1\cdots b_n \in \mathbb{Z}_p^n$ je kódové slovo, právě když splňuje rovnici*

$$b_1 + b_2 + \cdots + b_n = 0,$$

neb ta je splněna právě když kódové slovo obsahuje sudý počet jedniček. To ale znamená, že kódová slova jsou právě ty vektory, které jsou řešením homogenní soustavy s maticí

$$H_K = \begin{pmatrix}1 & 1 & 1 & \cdots & 1\end{pmatrix} \in \mathbb{Z}_p^{1,n}.$$

Frobeniova věta nám ale říká, že množina řešení homogenní soustavy[39] *je vždy podprostor. Takže ejhle: paritní kód je lineárním kódem! Frobeniova věta navíc říká, že dimenze řešení homogenní soustavy je rovna počtu proměnných (zde n) mínus hodnost matice H_K (zde zřejmě 1), můžeme upřesnit, že paritní kód je lineární $(n, n-1)$-kód obsahující 2^{n-1} kódových slov a mající $n-1$ informačních a 1 kontrolní znak.*

Matice H_K výše je tedy navíc kontrolní maticí[40] *a abychom získali nějakou generující, stačí najít bázi řešení homogenní soustavy s touto maticí, tedy soustavy*

$$\left(\begin{array}{ccccc|c}1 & 1 & 1 & \cdots & 1 & 0.\end{array}\right)$$

[38] A my už dávno víme, že přiřazení „vektor $\leftrightarrow$ jeho souřadnice ve zvolené bázi“ je vzájemně jednoznačné.

[39] Ve Frobeniově větě značená jako S_0.

[40] A označit ji H_K bylo tedy nanejvýš prozíravé!

Matice této soustavy už je v horním stupňovitém tvaru s jedním hlavním sloupcem (tím prvním) a $n-1$ vedlejšími. Bází množiny řešení je mnoho, jako celkem přirozená volba se nabízí tato:

$$((1,0,0,\ldots,0,1),(0,1,0,\ldots,0,1),(0,0,1,\ldots,0,1),\ldots,(0,0,0,\ldots,1,1))$$

tedy báze, jejích $j$tý člen obsahuje právě dvě jedničky: na $j$tém a $n$tém místě. Z této báze pak sestavíme generující matici

$$G_K = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 1 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 1 & \cdots & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \end{pmatrix}.$$

A s opakovacím kódem je to podobné, také je lineární:

Příklad 4.18. *Uvažujme opakovací kód K^3 z příkladu 4.2, který obsahuje slova ze $\mathbb{Z}_2^9$, která vzniknou trojím opakování třípísmenného binárního slova. Kódová slova poznáme tedy tak, že se rovnají jejich 1., 4. a 7. znak, stejně jako 2., 5. a 8. a 3., 6. a 9. znak. Jinými slovy, $b_1b_2\ldots b_9$ je kódové slovo jestliže je řešením následující homogenní soustavy*[41]

$$\left(H_{K^3} \mid \theta\right) = \left(\begin{array}{ccccccccc|c} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{array}\right).$$

Tedy i opakovací kód je opět roven množině řešení homogenní soustavy a tedy podprostor. Když si opět vezmeme na pomoc Frobeniovu větu a fakt, že matice H_{K^3} (což je kontrolní matice opakovacího kódu K^3) má hodnost 6, můžeme říci, že tento náš opakovací kód je lineární $(9,3)$-kód.

Generující matici můžeme volit všelijak, neb bází příslušného třídimenzionálního podprostoru je více, násl. matice je opět asi nejpřirozenější volbou:

$$G_{K^3} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Lineární kódy mohou i nemusí být systematické. Příklady těch systematických jsme si již uvedli: paritní i opakovací kód jsou systematické. Jako příklad nesystematického kódu můžeme vzít např. lineární $(5,2)$-kód z následujícího příkladu.

[41]Požadavek, aby se rovnaly 1., 4. a 7. znak slova $b_1b_2\cdots b_9$ vyžaduje dvě rovnice, např.: $b_1 = b_4$ a $b_4 = b_7$, proto má soustava celkem 6 rovnic. My je napsali v takovém pořadí, aby byla soustava v horním stupňovitém tvaru.

Příklad 4.19. *Uvažujme kód nad abecedou/tělesem $\mathbb{Z}_3$ s následující generující maticí*

$$G_K = \begin{pmatrix} 1 & 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

Tato matice je v horním stupňovitém tvaru a má zřejmě hodnost dva, soubor jejích řádků je tedy skutečně lineárně nezávislý a tvoří bázi nějakého dvoudimenzionálního podprostoru. Abychom získali všechna kódová slova, stačí vzít všechny lineární kombinace dvou bazických vektorů (tj. řádků generující matice) 10021 *a* 00110*. Takových lineárních kombinací je* $3^2 = 9$*, neboť těleso* $\mathbb{Z}_3$ *má tři prvky, existuje tedy právě devět kódových slov:*

$$00000, 10021, 20012, 00110, 00220, 10101, 20122, 10211, 20202.$$

Generující matici jsme dostali zadanou, jak získat matici kontrolní? Hledáme vlastně matici H_K *takovou, že množina řešení homogenní soustavy s touto maticí bude rovna podprostoru (tj. lineárnímu kódu)*

$$\langle 10021, 00110 \rangle.$$

Takové typy úloh už ale řešit umíme! Podprostor je varieta (za jejíž vektor posunutí můžeme volit nulový vektor) a hledat kontrolní matici je tak vlastně úloha hledání neparametrických rovnic variety! Přesný postup je dán důkazem Věty 3.41: víme, že hledaná matice bude mít $5 - 2 = 3$ *řádky a že tyto řádky můžeme volit jako jakékoli řešení homogenní rovnice s maticí, jejíž řádky jsou bazické vektory zaměření dané variety (zde podprostoru/lineárního kódu):*

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

To ale není nic jiného, než generující matice! Hledané tři vektory jsou například 20001*,* 10210 *a* 01000 *a jako kontrolní matici můžeme tedy vzít*

$$H_K = \begin{pmatrix} 2 & 0 & 0 & 0 & 1 \\ 1 & 0 & 2 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Lineární $(5, 2)$-kód z předchozího příkladu není systematický. Víme, že má 2 informační znaky a aby byl systematický, museli bychom při přečtení prvních dvou znaků všech jeho kódových slov dostat všech devět dvoupísmenných slov nad abecedou $\mathbb{Z}_3$. Kódová slova jsou ale tato:

$$00000, 10021, 20012, 00110, 00220, 10101, 20122, 10211, 20202.$$

a jejich první dva znaky nám tedy dávají množinu

$$00, 10, 20, 00, 00, 10, 20, 10, 20,$$

ve které chybí např. slovo 11.

Poznat, jestli je lineární kód systematický, je ale o něco jednodušší, známe-li jeho generující matici a následující větu.

Věta 4.20. *Lineární* (n,k)*-kód je systematický právě tehdy, když generující matici* ***lze volit*** *ve tvaru*

$$G_K = \begin{pmatrix} \mathbb{E} & \mathbb{A} \end{pmatrix},$$

kde $\mathbb{E}$ *je jednotková matice typu* $k \times k$ *a* $\mathbb{A}$ *nějaká matice typu* $k \times (n-k)$*.*

Než si větu dokážeme, zamyslíme se nad tím, co vlastně říká[42]. Zvolme si pro názornost za počet informačních znaků $k = 3$ a za abecedu $\mathbb{Z}_2$. Je-li kód systematický, tak množina třech prvních znaků všech slov je rovna množině $\mathbb{Z}_2^3$ a obsahuje tedy i slova 100, 010 a 001. V takovém kódu tedy existují tři kódová slova začínající právě těmito třemi znaky, označme si je[43] $u_1 = 100\cdots$, $u_2 = 010\cdots$, $u_3 = 001\cdots$. Snadno si rozmyslíte, že tato slova (chápána jako vektory) jsou lineárně nezávislá a tedy tvoří bázi třídimenzionálního podprostoru, který je zadaným systematickým lineárním $(n,3)$-kódem. No a co se nestane, když tyto tři vektory dosadíme do generující matice jako její řádky: dostaneme matici

$$G_K = \begin{pmatrix} 1 & 0 & 0 & \cdots \\ 0 & 1 & 0 & \cdots \\ 0 & 0 & 1 & \cdots \end{pmatrix}$$

jejíž první tři sloupce tvoří jednotkovou matici! A teď už je jistě pozorný čtenář připraven na řádný důkaz. Doporučujeme připomenout si definici 4.13 systematického kódu, která požaduje pro lineární (n,k)-kód nad $\mathbb{Z}_p$ existenci bijekce $\varphi : \mathbb{Z}_p^k \to K$ takové, že pro každé $u \in \mathbb{Z}_p^k$ existuje $v \in \mathbb{Z}_p^{n-k}$ pro které $\varphi(u) = uv$.

Důkaz. Buď K systematický lineární (n,k)-kód. Potom v něm existuje bijekce $\varphi : \mathbb{Z}_p^k \to K$ s výše popsanou vlastností. Buď $\mathcal{E} = (e_1, \ldots, e_k)$ standardní báze $\mathbb{Z}_p^k$. Pro všechna $i \in \hat{k}$ položme $\varphi(e_i) = e_i v_i$; dle definice jsou $e_i v_i$ kódová slova. Soubor těchto k slov je zřejmě lineárně nezávislý[44] a tvoří tedy bázi K. Z jejich konstrukce je navíc jasné, že když je pod sebe napíšeme v pořadí $e_1 v_1$, $e_2 v_2$, $\ldots e_k v_k$, dostaneme generující matici, jejíchž prvních k sloupců tvoří kýženou jednotkovou matici.

Pro důkaz implikace zprava doleva předpokládejme, že generující matice lineárního (n,k)-kódu K je

$$G_K = \begin{pmatrix} \mathbb{E} & \mathbb{A} \end{pmatrix},$$

pro nějakou matici $\mathbb{A}$. Hledanou bijekci mezi $\varphi : \mathbb{Z}_p^k \to K$ lze volit (podobně, jako v důkazu Věty 4.16) následovně: pro každé $u = u_1 u_2 \cdots u_k \in \mathbb{Z}_p^k$ položíme

$$\varphi(u) = (u_1 \; u_2 \; \cdots \; u_k) \cdot \begin{pmatrix} \mathbb{E} & \mathbb{A} \end{pmatrix} = uv^{45},$$

kde slovo v je vektor daný součinem

$$(u_1 \; u_2 \; \cdots \; u_k) \cdot \mathbb{A}.$$

□

[42]To je ostatně vhodné vždy!

[43]Tři tečky ... naznačují, že nás hodnota čtvrtého až $n$tého znaku kódových slov u_1, u_2 a u_3 nezajímají.

[44]Nebo snad lze jeden z těchto vektorů napsat jako lineární kombinací ostatních? Umíte to se standardní bází?

[45]Pod uv si zde musíme představit zřetězení slov u a v, tedy $n$tici, která je navíc napsaná do sloupečku. Opět si prosím podrobně promyslete, co přesně se děje při maticovém násobení výše.

Možná si říkáte, kam se nám poděl pojem nejmenší vzdálenost kódu a objevování/opravování chyb. Říkali jsme, že to je klíčová vlastnost kódu a teď o tom mlčíme. Zde si ukážeme, že zjistit minimální vzdálenost lineárního kódu je jednodušší, než u kódu v obecném případě. Obecně je třeba projít všechny dvojice kódových slov a pro každou dvojici spočítat Hammingovu vzdálenost. Pro lineární kód je to jednodušší, neb platí následující vlastnost plynoucí z uzavřenosti podprostoru vůči operacím vektorového prostoru: jsou-li u a v dvě kódová slova, je $u - v$ také kódové slovo. Než si ukážeme, jak tohoto využít k rychlejšímu určování minimální vzdálenosti kódu, definujme si následující pojem:

Definice 4.21. *Pro $u = u_1 u_2 \cdots u_n \in \mathbb{Z}_p^n$ definujeme* ***Hammingovu váhu*** *jako*

$$\|u\| = \text{ počet } i \in \hat{n} \text{ takových, že } u_i \neq 0,$$

tj. jako počet nenulových znaků ve slově u.

Představme-si, že u a v jsou dvě nejbližší kódová slova v lineárním kódu K; řekněme, že jejich vzdálenost je ℓ, což je tedy současně i minimální vzdálenost kódu K. Tato slova se liší právě v ℓ znacích a v ostatních se shodují. Jelikož K je lineární, je $u - v$ také kódové slovo. Jak toto kódové slovo vypadá? Na ℓ místech je má znak různý od nuly a na zbylých místech je nulové, dle definice je jeho váha rovna ℓ, což je současně minimální vzdálenost kódu.

No a jelikož Hammingova váha slova u je vlastně vzdálenost od nulového slova (nulového vektoru), který v lineárním kódu vždycky je[46], dokázali jsme vlastně následující:

Pozorování 4.22. *Buď K lineární kód.*

(i) Pro libovolné $u, v \in K$ platí

$$d(u, v) = \|u - v\|.$$

(ii) Minimální vzdálenost kódu je rovna minimální váze nenulového kódového slova, neboli

$$\mu(K) = \min\{\|u\| \mid u \in K, u \neq \theta\}.$$

Příklad 4.23 (pokračování)**.** *Výše jsme si ukázali lineární $(5, 2)$-kód s kódovými slovy*

$$00000, 10021, 20012, 00110, 00220, 10101, 20122, 10211, 20202.$$

Minimální vzdálenost tohoto kódu je rovna 2, neboť v něm jsou nenulová slova s váhou 2 a žádné slovo váhy 1. Tento kód tedy objevuje nejvýše jednu chybu a neopravuje žádnou.

Existuje ještě jeden způsob, jak zjistit minimální vzdálenost lineárního kódu: s využitím kontrolní matice a inspekcí jejích sloupců. Vezměme si kód z předchozího

[46]Fakt! V každém podprostoru je nulový vektor!

příkladu: nenulové kódové slovo s nejmenší váhou je např. 00220, kontrolní matice tohoto kódu je (viz výše)

$$H_K = \begin{pmatrix} 2 & 0 & 0 & 0 & 1 \\ 1 & 0 & 2 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Musí tedy platit, že

$$H_K \begin{pmatrix} 0 \\ 0 \\ 2 \\ 2 \\ 0 \end{pmatrix} = \theta.$$

Z toho je vidět, že lineární kombinace 3. a 4. sloupce s koeficienty 2 a 2 dává nulový vektor. To znamená, že soubor tvořený těmito vektory je lineárně závislý! No a toto pozorování lze zobecnit do následující věty:

Věta 4.24. *Lineární (n, k)-kód K objevuje, resp. opravuje t-chyby právě tehdy, když je soubor* ***libovolných*** *t, resp. $2t$ sloupců v jeho libovolné kontrolní matici H_K lineárně nezávislý.*

Důkaz. Tvrzení věty dokážeme pro objevování chyb, neb jde vlastně o minimální vzdálenost kódu a tvrzení bychom mohli přeformulovat[47] takto:

$$\mu(K) > t \Leftrightarrow \text{ soubor libovolných } t \text{ sloupců } H_K \text{ je LN.}$$

($\Rightarrow$): Implikaci dokážeme sporem. Uvažujme nejprve, že minimální vzdálenost je větší než t, ale existuje lineárně závislý soubor tvořený t sloupci nějaké kontrolní matice H_K. Označme indexy těchto sloupců j_1 až j_t a koeficienty příslušné netriviální lineární kombinace těchto sloupců jako $u_1, u_2, \ldots, u_t$ (jelikož je kombinace netriviální, existuje $i \in \hat{t}, u_i \neq 0$). Vytvořme slovo v délky n tak, že jeho písmeno na pozici j_i je rovno u_i pro všechna $i \in \hat{t}$ a všude jinde jsou nuly. Hammingova váha slova v je tedy nejméně 1 a nejvýše t, ovšem také platí, že (bereme-li v jako sloupcový vektor)

$$\sum_{i=1}^{t} u_i (H_K)_{:j_i} = \sum_{\ell=1}^{n} v_\ell (H_K)_{:\ell} = H_K \cdot (v_1 \; v_2 \; \cdots \; v_n)^T = H_K \cdot v\,,$$

kde první rovnost plyne z přidání nulových sčítanců do sumy a přeindexování (místo koeficientů $u_1, \ldots, u_t$ procházíme $n$tici získanou doplněním nulami) a druhá rovnost plyne ze základní vlastnosti maticového násobení – násobíme-li matici zprava sloupcovým vektorem v, vyrábíme lineární kombinace sloupců těchto matice s koeficienty v_ℓ.

V kódu K jsme tedy našli nenulové(!) kódové slovo v s $||v|| \leq t$, což je spor s předpokladem $\mu(K) > t$.

($\Leftarrow$): Důkaz druhé implikace je obdobný. Předpokládáme, že pro libovolnou kontrolní matici H_K platí, že libovolný soubor t jejích sloupců je LN a chceme dokázat, že $\mu(K) > t$. Budeme postupovat opět sporem, označíme-li $d := \mu(K)$, pro spor

[47] Skutečně, z definice platí „K opravuje t-chyby $\Leftrightarrow \mu(K) > 2t \Leftrightarrow K$ objevuje $2t$-chyby“.

předpokládejme, že $d \leq t$. Tedy v kódu existuje nějaké kódové slovo v, které je nenulové a má tuto minimální Hammingovu váhu d. To znamená, že existují indexy $i_1, \ldots, i_d \in \hat{n}$ takové, že v_{i_j} jsou nenulová písmena a na všech ostatních indexech má slovo v nulu.

Z definice kontrolní matice a vlastností maticového násobení pak dostáváme

$$v \in K \;\Leftrightarrow\; \theta = H_K \cdot (v_1 \cdots v_n)^T = \sum_{j=1}^{n} v_j (H_K)_{:j} = \sum_{l=1}^{d} \underbrace{v_{i_l}}_{\neq 0} (H_K)_{:l} \,.$$

Jelikož jsme nalezli netriviální lineární kombinaci d sloupců H_K rovnou nulovému vektoru, tento soubor musí být LZ. Nutně tedy platí $d > t$ (předpokládali jsme totiž, že každý soubor t sloupců (nebo menší) je LN) a dostáváme spor. $\square$

Předchozí věta nám pomůže z kontrolní matice poznat zejména kódy, jejichž minimální vzdálenost je hodně nízká. Platí totiž její následující triviální důsledky:

(i) Lineární kód má minimální vzdálenost jedna, právě když jeho kontrolní matice obsahuje nulový sloupec.

(ii) Lineární kód má minimální vzdálenost dva, právě když nějaký sloupec kontrolní matice je násobkem jiného.

4.4 Dekódování

Tato část textu bude doplněna posléze. Čtenáři proto doporučujeme, aby ke studiu tématu dekódování využil přednášky, prezentace k nim a také materiály ke cvičením – jako příprava na zkoušku budou naprosto postačující!

Kapitola 5

Lineární zobrazení

Pod pojmem *zobrazení* si typický čtenář pravděpodobně představí něco na způsob *reálné funkce reálné proměnné*, tedy to, co dobře zná například z kurzu BI–ZMA. V lineární algebře pojem zobrazení chápeme (v jistém smyslu) obecněji, jako relaci ne mezi reálnými čísly ale mezi vektory v libovolých vektorových prostorech. Aby té obecnosti nakonec nebylo příliš, omezíme se přitom na zobrazení, která jsou takzvaně *lineární*[1].

Valná část této kapitoly pak vlastně bude takovou malou propagací této vlastnosti, linearity. Podobně jako nám axiomy vektorového prostoru zaručují (ať už samy o sobě nebo svými důsledky) „rozumnou“ práci s vektory, linearita sama o sobě implikuje mnoho užitečných vlastností, díky kterým je život[2] snadnější a veselejší.

Lineární zobrazení je naprosto zásadní pojem lineární algebry a lze ho objevit v různých oblastech lidského konání. Asi nejnápadnější aplikace nalezneme v počítačové grafice, kde lineární zobrazení slouží například k transformacím obrazu (různé škálování, rotace, odrazy či projekce) nebo k vykreslování 3D scény v počítačových hrách[3]. S takovými zobrazeními jde navíc velice snadno pracovat, ukážeme si, že ke každému lineárními zobrazení lze sestavit takovou matici, která umožní nalezení obrazu libovolného vektoru jednoduchým vynásobením touto maticí!

Jak si dále ukážeme, i obyčejná soustava lineárních rovnic je vlastně speciálním případem rovnic tvaru $Ax = b$, kde A je lineární zobrazení, a všechno co o soustavách lineárních rovnic víme je do jisté míry důsledkem vlastností zobrazení[4]. Dalšími speciálními příklady jsou pak lineární rekurentní rovnice (pracujeme s nekonečnými posloupnostmi) nebo lineární diferenciální rovnice (pracujeme s funkcemi a jejich derivacemi), které díky lineární algebře lze řešit a které mají aplikace všude možně, od fyziky a elektroniky přes ekonomii až po medicínu.

5.1 Co si z této kapitoly odneseme

1. Zopakujeme si základní definice týkající se zobrazení a v kontextu lineární algebry zavedeme pojem *lineární zobrazení*.

[1] Aby taky ne, co jiného by se dalo v kurzu nazvaném *lineární* algebra čekat.
[2] Tedy práce s lineárními zobrazeními.
[3] Varování: předchozí věta obsahuje mistrný matematický marketing!
[4] Ano, hádáte dobře, největší zásluhy má právě linearita.

2. Důkladně rozpitváme linearitu a její různé důsledky. Zaměříme se přitom na další, u zobrazení oblíbené, vlastnosti – na injektivitu a surjektivitu.

3. Zavedeme si pojem matice lineárního zobrazení a ukážeme si, jak s ní pracovat. Naučíme se pracovat se souřadnicemi vektorů vzhledem k různým bázím namísto s vektory samotnými a převádět je z báze do báze.

4. Na příkladu prostoru bodů v rovině odvodíme různé druhy lineárních transformací.

5. Zamyslíme se nad řešitelností rovnic tvaru $Ax = b$ a uvedeme si příklady takových rovnic.

5.2 Základní pojmy

Jistě není od věci osvěžit si přesnou definici zobrazení a několik dalších základních pojmů. Jsou-li X a Y libovolné množiny, množinu uspořádaných dvojic

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}$$

nazýváme jejich **kartézským součinem**. Pak **zobrazením z** X **do** Y nazveme libovolnou podmnožinu $f \subseteq X \times Y$ takovou, že pro každé $x \in X$ existuje **nejvýše jedno** $y \in Y$ s vlastností $(x, y) \in f$. Používáme obvyklý zápis $f : X \to Y$ a skutečnost $(x, y) \in f$ zapisujeme tradičně jako $f(x) = y$.

- Platí-li $f(x) = y$, řekneme, že x je **vzorem** y a y je **obrazem** x při zobrazení f. Každý prvek z X má tedy nejvýše jeden obraz (jeden nebo žádný), ale každý prvek z Y může mít libovolný počet vzorů při zobrazení f.

- **Obrazem množiny** $M \subseteq X$ rozumíme množinu

  $$f(M) = \{f(a) \mid a \in M\},$$

  podobně **vzor množiny** $N \subseteq Y$ značíme

  $$f^{-1}(N) = \{a \in M \mid f(a) \in N\}.$$

  Pro obrazy a vzory jednoprvkových množin pak používáme zkrácené značení, $f(\{a\}) = f(a)$ a $f^{-1}(\{a\}) = f^{-1}(a)$.

- Zobrazení $f : X \to Y$ je **injektivní** (prosté), pokud $\forall x, y \in X : (f(x) = f(y) \Rightarrow x = y)$[5].

- Zobrazení $f : X \to Y$ je **surjektivní** (na), pokud $\forall y \in Y\ \exists x \in X : f(x) = y$, tedy pokud $f(X) = Y$[6].

[5]Oblíbená je také definice ve tvaru implikace ($x \neq y \Rightarrow f(x) \neq f(y)$). Čtenář znalý pojmu *obměněná implikace* zde nad existencí dvou „různých“ definic jistě nehne ani brvou.

[6]Častým omylem je záměna pojmů injektivní a surjektivní. Oba pochází z francouzštiny (respektive z latiny) a lze je chápat poměrně přímočaře. Zatímco injective znamená něco na způsob „vkládající dovnitř“, což prosté zobrazení v jistém smyslu dělá (každý prvek z X zobrazí na nějaký z Y a žádné dva se nezobrazí na stejný), prefix „sur-“ ve slově surjective pak přesně znamená ono české „na“ (obrazy prvků z X se zobrazí **na** celou množinu Y).

- Zobrazení $f : X \to Y$ je **bijektivní** (vzájemně jednoznačné), pokud je současně injektivní i surjektivní.
- Pro $f : Y \to Z$ a $g : X \to Y$ definujeme **složené** zobrazení $f \circ g : X \to Z$ předpisem $(f \circ g)(x) = f(g(x))$ pro všechna $x \in X$.
- Označme **identické** zobrazení na množině M jako id_M. Nechť $f : X \to Y$, pak zobrazení $g : Y \to X$ nazveme **inverzním zobrazením** k f, pokud platí $f \circ g = id_Y$ a $g \circ f = id_X$.

Poznámka 5.1. *Nejeden čtenář by si mohl po zopakování definic výše začít stýskat, chybí nám tam přeci pojmy definiční obor a obor hodnot! Není to vyloženě na škodu, v celém zbytku textu totiž budeme vždy pracovat s takzvanými* ***totálními*** *(všude definovanými) zobrazeními. Tedy takovými, kde* ***definičním oborem je celá množina*** X[7]*. Pojem* ***obor hodnot*** *se v textu dále pravděpodobně vyskytne, ale nebudeme pro něj zavádět speciální značení, vystačí nám zápis pomocí obrazu množiny,* $f(X)$*.*

5.3 Linearita a její důsledky

Definice 5.2. *Buďte* P *a* Q *dva vektorové prostory nad stejným tělesem* T*, nechť* $A : P \to Q$*. Zobrazení* A *nazveme* ***lineární*** *právě když současně platí:*

1. *(aditivita):* $\forall x, y \in P : A(x + y) = Ax + Ay$,
2. *(homogenita):* $\forall \alpha \in T, \forall x \in P : A(\alpha x) = \alpha Ax$.[8]

Množinu všech lineárních zobrazení z P *do* Q *značíme* $\mathcal{L}(P, Q)$*.*

Lineární zobrazení prostoru V *do* V *nazýváme* ***lineární operátor*** *(transformace) na* V*. Množinu všech lineárních operátorů na* V *značíme krátce* $\mathcal{L}(V)$*. Lineární zobrazení prostoru* V *do tělesa* T *nazýváme* ***lineární funkcionál*** *na* V*.*

Jak je patrno z předchozí definice, budeme u lineárních zobrazení používat značení mírně odlišné od například matematické analýzy. Rozdíly shrňme v poznámce.

Poznámka 5.3. *Oproti malým písmenům* $f, g, \ldots$ *budeme pro lineární zobrazení mezi vektorovými prostory používat písmena velká,* $A, B, \ldots$*. Navíc, nedojde-li tím ke zmatení, můžeme vypouštět některé závorky – obraz prvku* x *budeme moci značit nejen* $A(x)$*, ale také zkráceně jako* Ax*.*

V podobném duchu budeme zkracovat zápis složených zobrazení, namísto $A \circ B$ *lze psát pouze* AB*.*

Také se nenecháme zmást dvojím možným významem zápisu $A^{-1}(a)$*, který lze chápat jako „vzor prvku* a*“ (což je obecně množina) nebo jako „obraz prvku* a *při inverzním zobrazení* A^{-1}*“ (vždy jednoprvková množina). V textu budeme tento zápis defaultně chápat jako* ***vzor prvku****. Pokud bude navíc uvažované zobrazení* A *bijektivní, pak inverze* A^{-1} *existuje a obě možné interpretace zápisu* $A^{-1}(a)$ *splývají!*

[7] Tedy každý prvek $a \in X$ má **právě jeden** obraz v Y.

[8] Věnujme chvilku zamyšlení nad významem početních operací v obou požadovaných rovnostech! Aby bylo jasno, zatímco na levých stranách rovností sčítáme vektory a násobíme skalárem pomocí operací v prostoru P, sčítání a násobení napravo už probíhá ve vektorovém prostoru Q. Může tedy klidně jít o různá sčítání a různá násobení.

Pro ilustraci si uveďme několik jednoduchých příkladů lineárních zobrazení ve známých vektorových prostorech. Jejich linearitu si laskavý čtenář jistě pln nadšení ověří sám.

- $A : \mathbb{R} \to \mathbb{R}$,
$$Ax := \alpha x \text{ pro dané } \alpha \in \mathbb{R}\,,$$
- $B : \mathbb{C}^3 \to \mathbb{C}^2$,
$$B(x, y, z) := (x + 2y - z, x - 2y - 3z)\,,$$
- $C : T^\infty \to T^3$,
$$C(x_1, x_2, x_3, \dots) := (x_1, x_2, x_3)\,,$$
- $D : T^\infty \to T^\infty$,
$$D(x_1, x_2, x_3, \dots) := (x_2, x_3, x_4, \dots)\,,$$
- $E : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$,
$$E(x_1, x_2, \dots, x_{n-1}, x_n) := (x_2, x_3, \dots, x_n, x_1)\,,$$
- $F : \mathbb{R}^\infty \to \mathbb{R}^\infty$,
$$F(x_1, x_2, x_3, \dots) := (x_2 - x_1, x_3 - x_2, x_4 - x_3, \dots)\,,$$
- $G : \mathbb{R}^{2,2} \to \mathbb{R}^{2,2}$,
$$G\begin{pmatrix} a & b \\ c & d \end{pmatrix} := \begin{pmatrix} a+b & a-b \\ c-d & c+d \end{pmatrix}\,,$$
- Ve vektorovém prostoru $\mathcal{P}$ všech polynomů s operacemi sčítání polynomů a násobení polynomu číslem[9] je operace derivování lineárním zobrazením, tj. $H : \mathcal{P} \to \mathcal{P}$,
$$Hp = p'\,,$$
- *itý* souřadnicový funkcionál $x_i^\# : V_n \to T$ pro libovolný prostor V_n s bází $\mathcal{X} = (x_1, \dots, x_n)$.

Ovšem například zobrazení $I : \mathbb{R} \to \mathbb{R}$ definované předpisem $Ix = x + 1$ dle definice 5.2 lineární není[10]! Oproti tomu, v přiměřeně exotických vektorových prostorech může být lineární i zobrazení, od kterého bychom to asi nečekali, viz následující příklad.

Příklad 5.4. *Vzpomeňme na vektorový prostor z příkladu 2.10,* $(\mathbb{R}^+, \mathbb{R}, \oplus, \odot)$ *s operacemi definovanými*
$$x \oplus y := x \cdot y, \quad \alpha \odot x := x^\alpha.$$
Zobrazení $f : \mathbb{R}_+ \to \mathbb{R}$ *(zobrazuje z tohoto neobvyklého prostoru do standardního* $\mathbb{R}^1$*) s předpisem*
$$f(x) := \ln x$$
je lineární.

[9] Opravdu se jedná o vektorový prostor. Kdo nevěří, nechť si to dokáže.
[10] Ačkoli v kontextu matematické analýzy bychom ho nazvali lineární funkcí.

Lze snadno dokázat, že linearita zobrazení je ekvivalentní několika podobným vlastnostem, které mohou být užitečné při ověřování linearity nebo dále v této kapitole během různých navazujících důkazů.

Pozorování 5.5. *Buďte P a Q vektorové prostory nad T, nechť $A : P \to Q$. Následující tři tvrzení jsou ekvivalentní:*

(i) $A \in \mathcal{L}(P, Q)$.

(ii) $\forall \alpha \in T, \forall x, y \in P : A(\alpha x + y) = \alpha Ax + Ay$.

(iii) $\forall n \in \mathbb{N}, \forall \alpha_1, \dots, \alpha_n \in T, \forall x_1, \dots, x_n \in P :$

$$A\left(\sum_{i=1}^{n} \alpha_i x_i\right) = \sum_{i=1}^{n} \alpha_i A x_i \text{[11]}.$$

K důkazu tohoto pozorování vyzýváme samotného čtenáře[12]. Šikovným postupem je například dokázání *řetězce implikací*, například (*i*) $\Rightarrow$ (*ii*) $\Rightarrow$ (*iii*) $\Rightarrow$ (*i*), podobně jako při důkazu věty 3.17.

Laskavý čtenář pak může (náležitě rozcvičen právě provedeným důkazem) rovnou pokračovat důkazem dalšího pozorování, a to o linearitě inverzních a složených zobrazení.

Pozorování 5.6.

(i) *Je-li $A \in \mathcal{L}(P, Q)$ bijekce, potom existuje inverzní zobrazení A^{-1} a to je také lineární, tj.*

$$A^{-1} \in \mathcal{L}(Q, P).$$

(ii) *Buďte $A \in \mathcal{L}(P, Q)$ a $B \in \mathcal{L}(Q, R)$. Potom složené zobrazení BA definované předpisem $\forall x \in P : (BA)x = B(Ax)$ je také lineární, tj.*

$$BA \in \mathcal{L}(P, R)\,.$$

Bezprostředním důsledkem linearity zobrazení je několik zásadních vlastností. Například to, že lineární zobrazení *zachovávají* lineární obaly, že obrazy i vzory podprostorů jsou také podprostory nebo to, že v závislosti na „směru“ zachovávají lineární závislost nebo nezávislost souborů vektorů[13].

Věta 5.7. *Nechť $A \in \mathcal{L}(P, Q)$, kde P, Q jsou vektorové prostory nad T.*

(i) *Označíme-li nulové vektory v P a Q popořadě θ_P a θ_Q, platí*

$$A\theta_P = \theta_Q\,.$$

[11] Což lze bez nadsázky formulovat roztomilým jazykolamem *„(lineární) obraz lineární kombinace souboru vektorů je roven lineární kombinaci souboru (lineárních) obrazů těchto vektorů“* a tím například omračovat náhodné kolemjdoucí.

[12] Přesně v duchu hesla „těžko na cvičišti, lehko na bojišti“.

[13] Pokud si následující důkaz celý důkladně projdete, zjistíte, že kromě definice linearity nebo k ní ekvivalentních vlastností (pozorování 5.5) skutečně nic víc nepotřebujeme.

(ii) *Je-li $M \subseteq P$, potom*
$$A(\langle M \rangle) = \langle A(M) \rangle\,.$$

(iii) *Je-li $\tilde{P} \subset\subset P$, platí $A(\tilde{P}) \subset\subset Q$. Je-li $\tilde{Q} \subset\subset Q$, pak platí $A^{-1}(\tilde{Q}) \subset\subset P$.*

(iv) *Pro libovolné soubory $\mathcal{X} = (x_1, \dots, x_n)$ v P a $\mathcal{Y} = (y_1, \dots, y_n)$ v Q takové, že jeden je obrazem druhého (tj. $Ax_i = y_i$ pro každé $i \in \hat{n}$), platí: Je-li $\mathcal{X}$ LZ, pak i jeho obraz $\mathcal{Y}$ je LZ. Ekvivalentně: Pokud je $\mathcal{Y}$ LN, pak i jeho vzor $\mathcal{X}$ je LN.*

Důkaz. (i) Pro libovolné vektory $a \in P, b \in Q$ platí $0 \cdot a = \theta_P$ a $0 \cdot b = \theta_Q$. Tedy
$$A\theta_P = A(0 \cdot a) = 0 \cdot \underbrace{Aa}_{\in Q} = \theta_Q\,.$$

(ii) Nechť $y \in A(\langle M \rangle)$. Potom existuje $x \in \langle M \rangle$, že $Ax = y$. Jelikož $x \in \langle M \rangle$, existují $\alpha_1, \dots, \alpha_n \in T$ a $x_1, \dots, x_n \in M$ takové, že $x = \sum_{i=1}^n \alpha_i x_i$. Z linearity A dostáváme
$$y = Ax = A\left(\sum_{i=1}^n \alpha_i x_i\right) = \sum_{i=1}^n \alpha_i A x_i\,.$$
Vektor y je tedy lineární kombinací vektorů $Ax_1, \dots Ax_n$, nebo-li $y \in \langle A(M) \rangle$. Tím máme dokázanou inkluzi $A(\langle M \rangle) \subseteq \langle A(M) \rangle$. Opačnou inkluzi dokážeme snadno obdobně (v podstatě provedeme tytéž kroky, ale v obráceném pořadí), její důkaz proveďte sami jako cvičení.

(iii) Nejprve dokážeme, že obraz podprostoru je podprostor, nechť $\tilde{P} \subset\subset P$. Všimněme si, že $A(\tilde{P}) \neq \emptyset$, protože $\tilde{P} \neq \emptyset$. Dále jistě platí $A(\tilde{P}) \subseteq Q$. Stačí tedy ukázat
$$\forall \alpha \in T, \forall u, v \in A(\tilde{P}) : \alpha u + v \in A(\tilde{P})\,.$$
Pro libovolně volené $u, v \in A(\tilde{P})$ musí existovat vzory, tedy $x, y \in \tilde{P}$ splňující $u = Ax$ a $v = Ay$. Potom
$$\alpha u + v = \alpha Ax + Ay = A(\alpha x + y).$$
Protože $\tilde{P} \subset\subset P$, platí pro argument na pravé straně $\alpha x + y \in \tilde{P}$. Tedy nutně $\alpha u + v \in A(\tilde{P})$.

Dokažme, že vzor podprostoru je podprostor, nechť $\tilde{Q} \subset\subset Q$. Opět si všimněme, že $A^{-1}(\tilde{Q}) \neq \emptyset$, protože alespoň $\theta_P \in A^{-1}(\tilde{Q})$. Nechť $\alpha \in T$, $x, y \in A^{-1}(\tilde{Q})$. Potom $Ax \in \tilde{Q}$ a $Ay \in \tilde{Q}$. Protože platí $A(\alpha x + y) = \alpha Ax + Ay \in \tilde{Q}$, dostáváme, že $\alpha x + y \in A^{-1}(\tilde{Q})$.

(iv) Nechť $(x_1, \dots, x_n)$ je LZ soubor v P. Existují tedy koeficienty $\alpha_1, \dots, \alpha_n \in T$, které splňují $\sum_{i=1}^n \alpha_i x_i = \theta_P$ a současně existuje $j \in \hat{n}$ takové, že $\alpha_j \neq 0$. S využitím linearity a předchozích bodů dostáváme
$$\theta_Q = A\theta_P = A\left(\sum_{i=1}^n \alpha_i x_i\right) = \sum_{i=1}^n \alpha_i A x_i\,,$$
z čehož plyne, že soubor $(Ax_1, \cdots, Ax_n)$ je LZ.

Zbývá dokázat, že vzor libovolného LN souboru je také LN. Pro spor předpokládejme, že tvrzení neplatí, tedy že existuje nějaký LN soubor $(y_1, \ldots, y_n)$ z Q, jehož lineární vzor $(x_1, \ldots, x_n)$ je LZ. Při „obráceném" pohledu pak stačí jen konstatovat, že dostáváme spor s předchozím bodem. Skutečně, LZ soubor $(x_1, \ldots, x_n)$ by měl LN obraz a to není možné.

$\square$

Jak vyplývá z příkladů uvedených výše, lineární zobrazení mezi VP lze jistě definovat zadáním explicitního vzorečku[14]. Takový předpis je jistě šikovná věc, ale ne vždy ho máme k dispozici. Můžeme například dychtit po zobrazení, které několika konkrétním vektorům přiřadí zadané obrazy, ale jinak o něm nic dalšího nevíme. I zde nám linearita dává jistou naději. Jak shrnuje následující věta, stačí znát obrazy prvků nějaké báze prostoru P[15] a tím je už hledané zobrazení $A \in \mathcal{L}(P, Q)$ jednoznačně určeno!

Věta 5.8. *Nechť P, Q jsou vektorové prostory nad T. Nechť $(x_1, \ldots, x_n)$ je báze P a nechť $(y_1, \ldots, y_n)$ je libovolný soubor vektorů z Q. Potom existuje právě jedno lineární zobrazení $A \in \mathcal{L}(P, Q)$ takové, že*

$$\forall i \in \hat{n} : Ax_i = y_i .$$

Důkaz. Je-li soubor $(x_1, \ldots, x_n)$ bází P, pak každé $z \in P$ lze jednoznačně vyjádřit jako lineární kombinaci prvků této báze,

$$z = \sum_{i=1}^{n} \underbrace{x_i^{\#}(z)}_{\in T} x_i \text{[16]} .$$

Jelikož předpokládáme $Ax_i = y_i$ pro každé $i \in \hat{n}$, pak z linearity hledaného zobrazení plyne

$$A\left(\sum_{i=1}^{n} x_i^{\#}(z) x_i\right) = \sum_{i=1}^{n} x_i^{\#}(z) A x_i = \sum_{i=1}^{n} x_i^{\#}(z) y_i .$$

Tedy hledané zobrazení předepíšeme pomocí souřadnic v bázi $(x_1, \ldots, x_n)$ pravidlem

$$Az := \sum_{i=1}^{n} x_i^{\#}(z) y_i .$$

Je ovšem třeba zdůvodnit, že takto definované zobrazení $A : P \to Q$ je lineární. Potřebnou rovnost $A(\alpha u + v) = \alpha Au + Av$ pro libovolné vektory $u, v \in P$ a skalár $\alpha \in T$ lze však ověřit snadno s využitím linearity souřadnicových funkcionálů $x_i^{\#}$.

Zbývá ještě dokázat jednoznačnost, to provedeme sporem. Nechť existuje $B \in \mathcal{L}(P, Q)$ takové, že $\forall i \in \hat{n} : Bx_i = y_i$ a přitom $B \neq A$, tedy existuje vektor $a \in P$ takový, že $Ba \neq Aa$. Z linearity B ale dostáváme

$$Ba = B\left(\sum_{i=1}^{n} x_i^{\#}(a) x_i\right) = \sum_{i=1}^{n} x_i^{\#}(a) B x_i = \sum_{i=1}^{n} x_i^{\#}(a) y_i = Aa ,$$

[14] Máme na mysli funkční předpis ve tvaru: „pro libovolné $x \in P$ platí $Ax = \ldots$".

[15] U kterého budeme tiše předpokládat konečnou dimenzi – v zájmu obecného blaha a jednoduššího důkazu.

[16] Podržme minutu ticha za všechny, kteří si mysleli, že souřadnicový funkcionál už ve zbytku tohoto textu nepotkají.

což je spor. $\square$

Příklad 5.9. *Uvažujme zobrazení $A : \mathbb{R}^3 \to \mathbb{R}^4$ zadané obrazy prvků standardní báze*[17]*,*

$$Ae_1 = (1, 0, 1, -1), \quad Ae_2 = (0, 0, 1, 1), \quad Ae_3 = (0, 3, -1, 0)\,.$$

Jelikož pro každý vektor $z = (a, b, c) \in \mathbb{R}^3$ platí $z = ae_1 + be_2 + ce_3$, dostáváme

$$\begin{aligned} Az &= A(ae_1 + be_2 + ce_3) \\ &= aAe_1 + bAe_2 + cAe_3 \\ &= a(1, 0, 1, -1) + b(0, 0, 1, 1) + c(0, 3, -1, 0) \\ A(a, b, c) &= (a, 3c, a + b - c, -a + b)\,. \end{aligned}$$

Příklad 5.10. *Uvažujme zobrazení $B : \mathbb{R}^3 \to \mathbb{R}^4$ zadané obrazy prvků báze $\mathcal{X} = (x_1, x_2, x_3)$, kde*

$$x_1 = (1, 0, 0), \quad x_2 = (1, 1, 0), \quad x_3 = (1, 1, 1)\,,$$

$$Bx_1 = (1, 1, 1, 1), \quad Bx_2 = (0, 1, 0, -1), \quad Bx_3 = (0, 0, 1, -1)\,.$$

Abychom mohli odvodit předpis pro zobrazení B, musíme nejdříve určit souřadnice obecného vektoru $z = (a, b, c) \in \mathbb{R}^3$ v bázi $\mathcal{X}$. Jak si čtenář milerád sám ověří, rovnice

$$z = (a, b, c) = \alpha(1, 0, 0) + \beta(1, 1, 0) + \gamma(1, 1, 1)$$

má řešení

$$x_1^{\#}(z) = \alpha = a - b, \quad x_2^{\#}(z) = \beta = b - c, \quad x_3^{\#}(z) = \gamma = c\,.$$

Pak už podobně jako v předchozím příkladu odvodíme

$$\begin{aligned} Bz &= B\big((a - b)x_1 + (b - c)x_2 + cx_3\big) \\ &= (a - b)Bx_1 + (b - c)Bx_2 + cBx_3 \\ &= (a - b)(1, 1, 1, 1) + (b - c)(0, 1, 0, -1) + c(0, 0, 1, -1) \\ B(a, b, c) &= (a - b, a - c, a - b + c, a - 2b)\,. \end{aligned}$$

Poznámka 5.11. *Přijdou vám postupy v příkladech 5.9 a 5.10 příliš technické, nepřehledné či komplikované? Nezoufejte! V části 5.5* Matice lineárního zobrazení *si vyložíme mnohem elegantnější a praktičtější způsob, jak takovéto úlohy řešit. Kromě špetky logického uvažování přitom nebudeme potřebovat skoro nic kromě maticového násobení, hledání inverzí a řešení soustav lineárních rovnic – což je pro nás už samozřejmě rutina…*

[17] $e_1 = (1, 0, 0), e_2 = (0, 1, 0), e_3 = (0, 0, 1)$.

5.4 Hodnost, jádro a defekt zobrazení

Definice 5.12. *Nechť $A \in \mathcal{L}(P,Q)$.* ***Hodností zobrazení*** *A rozumíme číslo*

$$h(A) := \dim A(P)\,.$$

Jádro zobrazení *A definujeme jako množinu*

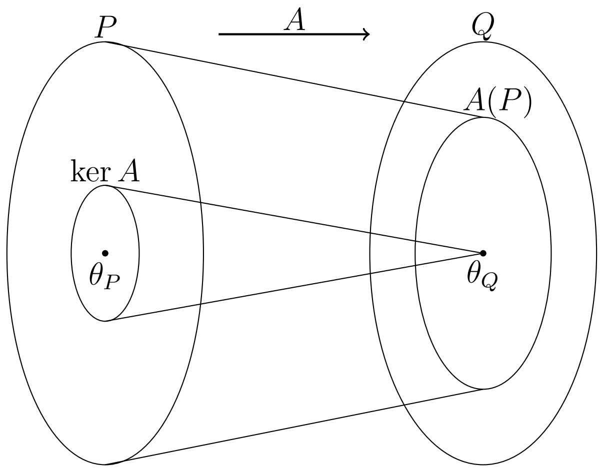
$$\ker A := \{x \in P \mid Ax = \theta_Q\}\,,$$

a jeho dimenzi nazýváme ***defektem zobrazení*** *A. Defekt značíme*

$$d(A) := \dim \ker A\,.$$

Poznamenejme, že právě zavedené pojmy opravdu dávají smysl. Z věty 5.7 totiž plyne, že obor hodnot $A(P)$ i jádro $\ker A = A^{-1}(\theta_Q)$[18] jsou podprostory. Má tedy smysl mluvit o jejich dimenzích.

Pokusíme se zde ještě odvrátit jedno časté studentské faux pas, a to zdůrazněním, že *hodnost zobrazení* je **odlišný pojem** od *hodnosti matice*! I když si v budoucnu těsný[19] vztah mezi těmito pojmy popíšeme, musíme je rozlišovat!



Obrázek 5.1: Ilustrace jádra a oboru hodnot pro $A \in \mathcal{L}(P,Q)$.

Příklad 5.13. *Odvodíme jádra lineárních zobrazení uvedených na začátku kapitoly. Ve všech případech je třeba vyřešit rovnici $Ax = \theta$, kde za x dosadíme obecný vektor v daném prostoru a za θ příslušný nulový vektor. To vždy povede na nějakou soustavu lineárních rovnic*[20]*, kterou snadno vyřešíme. Pro první tři příklady zobrazení uveďme celý postup řešení:*

[18] Jde o vzor jednoprvkové množiny $\{\theta_Q\}$, která je triviálním podprostorem.
[19] Až téměř intimní.
[20] Jak překvapivé!

- *$A:\mathbb{R}\to\mathbb{R}$, $Ax := \alpha x$ pro $\alpha\in\mathbb{R}$:*

  Je-li $\alpha = 0$, pak rovnice $\alpha x = 0$ platí pro libovolný vektor $x\in\mathbb{R}$. Je-li naopak $\alpha\neq 0$, pak platí $\alpha x = 0 \Rightarrow x = 0$. Tedy

$$\ker A = \begin{cases} \{0\} = \{\theta_{\mathbb{R}}\} & \text{pro } \alpha\neq 0\,, \\ \mathbb{R} & \text{pro } \alpha = 0\,. \end{cases}$$

- *$B:\mathbb{C}^3\to\mathbb{C}^2$, $B(x,y,z) := (x+2y-z, x-2y-3z)$:*

  Rovnice $B(x,y,z) = \theta_{\mathbb{C}^2} = (0,0)$ vede na soustavu dvou lineárních rovnic,

$$\begin{aligned} x+2y-z &= 0, \\ x-2y-3z &= 0, \end{aligned}$$

  kterou hravě vyřešíme, řešením je $(x,y,z)\in\langle(4,-1,2)\rangle$. Tedy

$$\ker B = \langle(4,-1,2)\rangle\,.$$

- *$C:T^\infty\to T^3$, $C(x_1,x_2,x_3,\dots) := (x_1,x_2,x_3)$:*

  Rovnost $C(x_1,x_2,x_3,\dots) = \theta_{T^3} = (0,0,0)$ vede na triviální rovnice $x_1 = x_2 = x_3 = 0$, tedy v jádru zobrazení C jsou všechny nekonečné posloupnosti, které začínají trojicí nul,

$$\ker C = \{(0,0,0,x_4,x_5,\dots) \mid \forall i\geq 4 : x_i\in T\}\,.$$

Nalezení jader ostatních zobrazení ponecháváme na čtenáři jako cvičení:

- *$D:T^\infty\to T^\infty$, $D(x_1,x_2,x_3,\dots) := (x_2,x_3,x_4,\dots)$,*
- *$E:\mathbb{Z}_2^n\to\mathbb{Z}_2^n$, $E(x_1,x_2,\dots,x_{n-1},x_n) := (x_2,x_3,\dots,x_n,x_1)$,*
- *$F:\mathbb{R}^\infty\to\mathbb{R}^\infty$, $F(x_1,x_2,x_3,\dots) := (x_2-x_1, x_3-x_2, x_4-x_3,\dots)$,*
- *$G:\mathbb{R}^{2,2}\to\mathbb{R}^{2,2}$, $G\begin{pmatrix} a & b \\ c & d\end{pmatrix} := \begin{pmatrix} a+b & a-b \\ c-d & c+d\end{pmatrix}$,*
- *derivující zobrazení $H:\mathcal{P}\to\mathcal{P}$, $Hp = p'$ ve vektorovém prostoru polynomů $\mathcal{P}$,*
- *itý souřadnicový funkcionál $x_i^\#:V_n\to T$ pro libovolný prostor V_n s bází $\mathcal{X} = (x_1,\dots,x_n)$.*

Pro lepší pochopení pojmů hodnost a defekt lineárního zobrazení (a souvislosti mezi nimi) je klíčová tzv. **druhá věta o dimenzi**. Pro větší složitost však její důkaz neuvádíme a nebude ani vyžadován.

Věta 5.14 (2. o dimenzi)**.** *Nechť $A\in\mathcal{L}(P,Q)$. Potom*

$$h(A) + d(A) = \dim P.$$

Injektivita a surjektivita zobrazení

Jistě dobře víme, jak ověřit, zda je zadané zobrazení injektivní (prosté), i u lineárních zobrazení mezi vektorovými prostory by standardní postup přímo z definice[21] jistě fungoval. My na to ovšem půjdeme jinak a jednodušeji! Využijeme (opět) linearity zobrazení a z ní plynoucího vztahu mezi injektivitou zobrazení a jeho jádrem.

Věta 5.15. *Nechť $A \in \mathcal{L}(P, Q)$. Potom platí:*

$$A \text{ je prosté } \Leftrightarrow \ker A = \{\theta_P\}\,.$$

Důkaz.
$(\Rightarrow)$: Víme, že $A\theta_P = \theta_Q$. Protože A je prosté, neexistuje jiný vektor než θ_P, které by A zobrazilo na θ_Q. Tedy, $\ker A = \{\theta_P\}$.

$(\Leftarrow)$: Připomeňme, že $A \in \mathcal{L}(P, Q)$ je prosté právě když

$$\forall x, y \in P : (Ax = Ay \Rightarrow x = y)\,.$$

Nechť tedy nějaké $x, y \in P$ splňují rovnost $Ax = Ay$. Potom $Ax - Ay = \theta_Q$ a s využitím linearity dostáváme $A(x - y) = \theta_Q$. To znamená, že $x - y \in \ker A = \{\theta_P\}$. Tudíž $x - y = \theta_P$, neboli $x = y$. ☐

Z vět 5.14 a 5.15 můžeme rovnou odvodit jednoduchý vztah mezi injektivitou lineárního zobrazení, hodností a defektem. K němu přidáme i podobně přímočaré pozorování pro surjektivitu. Přitvrdíme-li pak předpokladem stejné konečné dimenze prostorů P a Q, zjistíme, že injektivita a surjektivita spolu souvisí těsněji, než by se na první pohled zdálo.

Pozorování 5.16. *Nechť $A \in \mathcal{L}(P, Q)$ a dimenze $\dim P$ a $\dim Q$ jsou konečné*[22].

- *A je injektivní* $\Leftrightarrow \ker A = \{\theta_P\} \Leftrightarrow d(A) = 0 \Leftrightarrow h(A) = \dim P$,
- *A je surjektivní* $\Leftrightarrow A(P) = Q \Leftrightarrow$[23] $\dim A(P) = \dim Q \Leftrightarrow h(A) = \dim Q$.

Důsledek 5.17. *Nechť $n \in \mathbb{N}$ a $A \in \mathcal{L}(P_n, Q_n)$. Pak je A injektivní právě tehdy, když je surjektivní.*

Důkaz. Jelikož $\dim P_n = \dim Q_n = n < \infty$, platí

$$A \text{ je prosté} \Leftrightarrow \ker A = \{\theta_{P_n}\} \Leftrightarrow d(A) = 0 \Leftrightarrow h(A) = n \Leftrightarrow A(P_n) = Q_n \Leftrightarrow A \text{ je na}\,.$$

☐

V jedné z části věty 5.7 jsme si dokázali, že lineární zobrazení částečně zachovávají lineární (ne)závislost, konkrétně že obraz každého LZ souboru je LZ a vzor každého LN souboru je LN. Je-li lineární zobrazení navíc injektivní, pak toto „zachovávání“ funguje i druhým směrem.

[21] Tedy ověření, zda $Ax = Ay$ implikuje $x = y$.

[22] Tento předpoklad je nutný pro platnost pouze některých směrů dvou z ekvivalencí níže. Zkuste je najít!

[23] Kontrolní otázka: zatímco rovnost $A(P) = Q$ zjevně implikuje rovnost dimenzí, proč to platí i obráceně?

Věta 5.18. *Nechť $A \in \mathcal{L}(P, Q)$ je prosté. Potom*

(i) je-li $(y_1, \ldots, y_n)$ LZ soubor vektorů z $A(P)$, je také soubor vzorů $(x_1, \ldots, x_n)$ LZ (tedy předpokládáme že $\forall i \in \hat{n} : y_i = Ax_i$).

(ii) je-li $(x_1, \ldots, x_n)$ LN soubor vektorů z P, je také $(Ax_1, \ldots, Ax_n)$ LN.

Důkaz. (i) Je-li $(y_1, \ldots, y_n)$ LZ soubor vektorů z Q, existují $\alpha_1, \ldots, \alpha_n \in T$ a $j \in \hat{n}$, že $\alpha_j \neq 0$ takové, že

$$\theta_Q = \sum_{i=1}^{n} \alpha_i y_i = \sum_{i=1}^{n} \alpha_i A x_i = A\left(\sum_{i=1}^{n} \alpha_i x_i\right).$$

Tedy platí $\sum_{i=1}^{n} \alpha_i x_i \in \ker A$. Jelikož je ale A z předpokladu prosté, platí $\ker A = \{\theta_P\}$ a rovnost $\sum_{i=1}^{n} \alpha_i x_i = \theta_P$ implikuje, že soubor $(x_1, \ldots, x_n)$ je LZ.

(ii) Kdyby existoval LN soubor, jehož obraz by byl LZ, dostali bychom se do sporu s bodem (i).

$\square$

Důsledek 5.19. *Nechť $A \in \mathcal{L}(P, Q)$ je prosté. Pokud soubory $(x_1, \ldots, x_n)$ v P a $(y_1, \ldots, y_n)$ v Q splňují $Ax_i = y_i$ pro každé $i \in \hat{n}$, pak platí*

$$(x_1, \ldots, x_n) \text{ je LN } \Leftrightarrow (y_1, \ldots, y_n) \text{ je LN}.$$

Definice 5.20. *Buď V vektorový prostor. Zobrazení $E : V \to V$ definované vztahem*

$$\forall x \in V : Ex = x$$

*je lineární operátor a nazýváme ho **identický operátor na** V.*

Izomorfismem *nazveme jakékoli zobrazení $A \in \mathcal{L}(P, Q)$, které je současně bijekce*[24]*.*

Omezíme-li se v našich úvahách na lineární operátory, tedy na lineární zobrazení na jednom vektorovém prostoru, lze o injektivitě a surjektivitě rozhodnout i podle jiného kritéria, než jaká doposud známe. Nejen v matematické analýze jsme už jistě slyšeli, že zobrazení je bijekce právě tehdy, když k němu existuje zobrazení inverzní. To platí i v lineární algebře a navíc lze formulovat i „podobné“ zákonitosti pro zobrazení pouze prostá, nebo pouze „na“.

Věta 5.21. *Buď $A \in \mathcal{L}(V)$.*

(i) Existuje-li $B \in \mathcal{L}(V)$ takový, že $AB = E$, pak je A surjektivní.

(ii) Existuje-li $C \in \mathcal{L}(V)$ takový, že $CA = E$, pak je A injektivní.

[24] Pojmem izomorfismus se dále nebudeme moci příliš zabývat (z prostorových důvodů). I přesto se ale jedná o důležitý pojem, povědomí o něm považujme za jakési civilizační minimum. Člověk nikdy neví, kdy se ho na definici izomorfismu někdo zeptá, ať už v tramvaji nebo například u státnic.

(iii) Jsou-li splněny předpoklady bodu (i) ***a zároveň*** *(ii), potom je A bijekce (tedy izomorfismus) a platí*

$$B = C = A^{-1}\,.$$

(iv) Je-li dimenze $\dim V < \infty$ a jsou-li splněny předpoklady bodu (i) ***nebo*** *(ii), potom je A bijekce a zobrazení B nebo C z předpokladu je rovno A^{-1}.*

Důkaz.

(i) Chceme dokázat, že $\forall y \in V, \exists x \in V : y = Ax$. Zvolme tedy libovolné $y \in V$. Hledané $x \in V$ rovnou definujme, a to jako $x := By$. Potom rovnou platí

$$Ax = A(By) = (AB)y = Ey = y\,.$$

(ii) Ukážeme, že $\ker A = \{\theta\}$. Nechť $x \in \ker A$, pak $Ax = \theta$. Odtud pak rovnou dostáváme:

$$x = Ex = (CA)x = C(Ax) = C\theta = \theta\,,$$

tedy každý vektor v $\ker A$ je nutně nulový.

(iii) A je z bodů (i) a (ii) prosté i „na“, je to tedy bijekce a existuje inverzní zobrazení A^{-1}. Musíme ukázat, že zobrazení B, C se této inverzi rovnají. Rovnost $B = A^{-1}$ odvodíme snadno,

$$A^{-1} = A^{-1}E = A^{-1}(AB) = (A^{-1}A)B = EB = B.$$

Druhou z rovností, $C = A^{-1}$, lze snadno dokázat obdobně, jak se laskavý čtenář jistě rád přesvědčí.

(iv) Plyne z předchozích bodů a z důsledku 5.17.

□

Na závěr této části napravíme hřích z dřívějška. V části 3.3 jsme totiž čtenáře okradli o důkaz jedné důležité věty, konkrétně šlo o větu 3.14 o regularitě matice:

Buď $\mathbb{A} \in T^{n,n}$. Existuje-li $\mathbb{B} \in T^{n,n}$ taková, že platí $\mathbb{AB} = \mathbb{E}$ nebo $\mathbb{BA} = \mathbb{E}$, potom je $\mathbb{A}$ regulární a $\mathbb{B} = \mathbb{A}^{-1}$.

Tuto mezeru doplníme až nyní, dříve jsme neměli k dispozici potřebné pojmy a tvrzení, současně půjde o jakýsi oslí můstek k následující části 5.5 *Matice lineárního zobrazení*. V důkazu totiž použijeme důležitou souvislost mezi lineárními zobrazeními a maticemi, o které v podstatě celá následující část kapitoly bude.

Důkaz věty 3.14. K libovolné matici $\mathbb{A} \in T^{n,n}$ definujme zobrazení $A : T^n \to T^n$ předpisem

$$\forall \mathbb{x} \in T^n : A\mathbb{x} := \mathbb{A} \cdot \mathbb{x},$$

kde $\mathbb{x} \in T^n$ je chápán jako sloupcový vektor (násobení $\mathbb{A} \cdot \mathbb{x}$ tedy má smysl). Díky distributivnímu zákonu pro maticové násobení je toto zobrazení lineární, tedy $A \in \mathcal{L}(T^n)$. Navíc, zavedeme-li podobně pro matici $\mathbb{B}$ zobrazení B, platí[25] i

[25] Vše si, spolu s linearitou, tréninkově rozmyslete!

- $A = B \Leftrightarrow \mathbb{A} = \mathbb{B}$
- matici $\mathbb{AB}$ odpovídá složené zobrazení AB, neboť pro libovolné $\mathbb{x} \in T^n$ platí $(AB)\mathbb{x} = A(B\mathbb{x}) = \mathbb{A}(\mathbb{B}\mathbb{x}) = (\mathbb{AB})\mathbb{x}$,
- jednotkové matici $\mathbb{E}$ odpovídá identické zobrazení E na T^n.

Nyní můžeme přistoupit k samotnému důkazu věty.

(i) Nechť existuje $\mathbb{B} \in T^{n,n}$ taková, že platí $\mathbb{AB} = \mathbb{E}$. Odtud máme rovnost příslušných zobrazení $AB = E$. Protože je $\dim T^n < \infty$, plyne z věty 5.21, že A je bijekce a pro jeho inverzi platí $A^{-1} = B$. Tedy také $BA = E$, což pro odpovídající matice dává druhou rovnost $\mathbb{BA} = \mathbb{E}$. Máme tedy obě rovnosti: $\mathbb{AB} = \mathbb{BA} = \mathbb{E}$.

(ii) Předpokládáme-li, že existuje $\mathbb{B} \in T^{n,n}$ taková, že $\mathbb{BA} = \mathbb{E}$, dostaneme postupem analogickým tomu z bodu (i), že i $\mathbb{AB} = \mathbb{E}$.

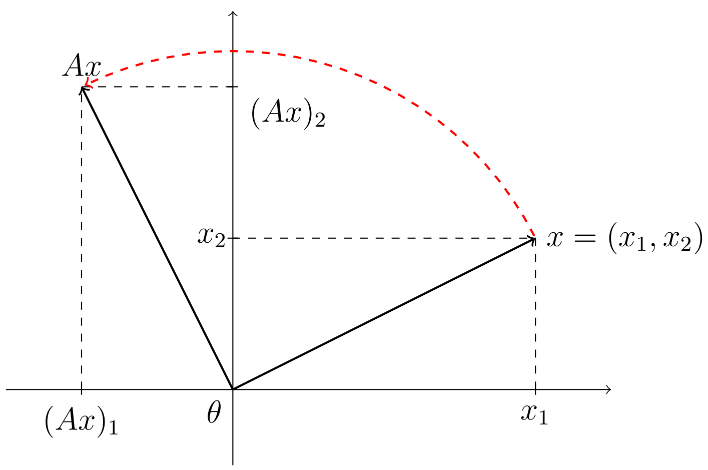
$\square$

5.5 Matice lineárního zobrazení

Jak jsme již naznačili v poznámce 5.11, zatím nám zoufale chybí nějaký jednoduchý nástroj pro práci se zobrazeními, k hledání obrazů nebo vzorů, ke skládání zobrazení nebo jeho invertování. Tím bude zavedení matice zobrazení.

Motivace

Začněme pro ilustraci jednoduchým příkladem, nechť $V = \mathbb{R}^2$, na něm uvažujme operátor $A \in \mathcal{L}(\mathbb{R}^2)$, který s každým vektorem (bodem v rovině, resp. šipkou z počátku) provede „rotaci okolo počátku o úhel $\frac{\pi}{2}$“[26].



[26] V kladném smyslu, tedy proti směru hodinových ručiček.

Vzpomeneme-li si na základy rovinné geometrie, jistě snadno odvodíme, že takové otočení o pravý úhel zobrazí každý bod podle předpisu

$$(x_1, x_2) \xrightarrow{A} (-x_2, x_1)\,,$$

ale použitelnost takové „vykoukávací“ metody je samozřejmě omezená jen na podobně triviální příklady.

Pozorný čtenář si jistě vzpomene na větu 5.8, která říkala, že lineární zobrazení lze jednoznačně určit obrazy nějaké báze. Obecně je jistě snazší nalézt obrazy několika konkrétních vektorů namísto odvození obrazu vektoru obecného[27]. Zvolme standardní bázi $\mathbb{R}^2$, $\mathcal{E} = (e_1, e_2) = ((1,0),(0,1))$. Pak platí

$$Ae_1 = A(1,0) = (0,1) = e_2\,, \quad Ae_2 = A(0,1) = (-1,0) = -e_1\,.$$

V důkazu věty 3.14 provedeném na konci části 5.4 jsme ke čtvercové matici $\mathbb{A}$ definovali lineární zobrazení A na prostoru sloupcových vektorů pravidlem $A\mathbb{x} = \mathbb{A}\mathbb{x}$, pokusme se teď o krok opačným směrem. Hledáme tedy matici

$$\mathbb{A} \in \mathbb{R}^{2,2} \text{ takovou, že platí } \forall \mathbb{x} \in \mathbb{R}^2 : \mathbb{A}\mathbb{x} = A\mathbb{x}\,.$$

1. Známe-li obraz obecného vektoru $A\mathbb{x}$, stačí dosadit do rovnice výše. Tedy hledáme matici $\mathbb{A} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ takovou, že pro každý $\mathbb{x} = (x_1\ x_2)^T \in \mathbb{R}^2$ platí

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -x_2 \\ x_1 \end{pmatrix}\,,$$

   tedy

$$\begin{aligned} \alpha x_1 + \beta x_2 &= -x_2\,, \\ \gamma x_1 + \delta x_2 &= x_1\,. \end{aligned}$$

   Jelikož rovnosti výše mají platit pro libovolné hodnoty $x_1, x_2 \in \mathbb{R}$, dostáváme $\alpha = \delta = 0, \beta = -1, \gamma = 1$, tedy rotaci vektorů v rovině (napsaných do sloupce) o pravý úhel můžeme realizovat násobením zleva maticí

$$\mathbb{A} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\,.$$

2. Ze znalosti obrazů vektorů standardní báze lze matici příslušnou k zadanému zobrazení také odvodit. Poznamenejme nejdříve, že pro libovolné $n \geq 1$ a matici $\mathbb{A} \in T^{n,n}$ platí, že její sloupce lze získat vynásobením se sloupcovými vektory standardní báze T^n, tedy že pro každé $j \in \hat{n}$ platí

$$\mathbb{A}\mathbb{e}_j = \mathbb{A}_{:j}\text{[28]}\,.$$

   Jelikož v našem případě platí $n = 2$, $A(1,0) = (0,1)$ a $A(0,1) = (-1,0)$, stačí tyto obrazy bazických vektorů zapsat do sloupců a stejně jako v bodě 1 dostáváme $\mathbb{A} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

[27] I když u tohoto zobrazení jde o porovnatelně „obtížné“ kroky.

[28] Což si rozhodně neváhejte ověřit! K tomu postačí předpis pro maticové násobení a popis složek jednotkových vektorů $\mathbb{e}_i$ pomocí symbolu Kroneckerovo delta δ_{ij} (z poznámky 2.71).

Nalezenou matici $\mathbb{A}$ budeme posléze sofistikovaněji nazývat *matice zobrazení A ve standardní bázi*[29]. Důvod k tomuto označení je zřejmý, vynásobíme-li maticí $\mathbb{A}$ sloupec souřadnic vektoru ve standardní bázi (to je ono $\mathbb{x}$), dostaneme přesně obraz tohoto vektoru při zobrazení A, ovšem opět zapsaný sloupečkem souřadnic. Matice $\mathbb{A}$ přitom ve svých sloupcích obsahuje právě obrazy vektorů standardní báze zapsané svými souřadnicemi ve standardní bázi[30].

Naše potřeby nicméně půjdou o kousek dále, možnost pracovat v souřadnicích ve standardní bázi (což je ve VP T^n totéž, jako s vektory samotnými) nám nebude vždy stačit. Proto zavedeme pojem *matice zobrazení v bázích* obecněji. A to tak, že pro libovolnou dvojici bází $\mathcal{X}$, $\mathcal{Y}$ prostorů P, resp. Q budeme toužit po matici $\mathbb{A}$ takové, že

- vynásobením sloupce souřadnic vektoru v bázi $\mathcal{X}$ maticí $\mathbb{A}$ zleva získáme rovnou jeho obraz, a to zapsán sloupcem souřadnic v bázi $\mathcal{Y}$,
- hledání vzoru vektoru při zobrazení A realizujeme řešením soustavy s maticí levé strany $\mathbb{A}$ a pravou stranou rovnou souřadnicím tohoto vektoru v bázi $\mathcal{Y}$. Množinu řešení soustavy pak budeme interpretovat jako souřadnice hledaných vzorů v bázi $\mathcal{X}$.

Abychom ještě lépe ospravedlnili potřebu pracovat se souřadnicemi vektorů a ne přímo s vektory, zamyslíme se, jak to s odvozením matice zobrazení funguje v jiných prostorech než v T^n.

Příklad 5.22. *Nechť $V = \mathbb{R}^{2,2}$, uvažujme lineární operátor $A \in \mathcal{L}(\mathbb{R}^{2,2})$ definovaný předpisem*

$$A \begin{pmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{pmatrix} := \begin{pmatrix} x_{1,1} + x_{1,2} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{pmatrix}$$

pro každé $x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2} \in \mathbb{R}$[31].

Pokud by existovala matice $\mathbb{A}$ taková, aby pro libovolnou matici $\mathbb{X} = \begin{pmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{pmatrix}$ platilo $A\mathbb{X} = \mathbb{A}\mathbb{X}$, musela by nutně[32] *být typu 2×2, tedy $\mathbb{A} \in \mathbb{R}^{2,2}$. Pokusme se takovou matici najít, nechť $\mathbb{A} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, pak pro libovolnou volbu parametrů $x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2} \in \mathbb{R}$ musí platit*

$$\mathbb{A}\mathbb{X} = A\mathbb{X} \quad \Leftrightarrow \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot \begin{pmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{pmatrix} = \begin{pmatrix} x_{1,1} + x_{1,2} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{pmatrix},$$

což vede na soustavu lineárních rovnic

$$\begin{aligned} \alpha x_{1,1} + \beta x_{2,1} &= x_{1,1} + x_{1,2} \\ \alpha x_{1,2} + \beta x_{2,2} &= x_{1,2} \\ \gamma x_{1,1} + \delta x_{2,1} &= x_{2,1} \\ \gamma x_{1,2} + \delta x_{2,2} &= x_{2,2}\,. \end{aligned}$$

[29] Nebo lépe: ze standardní báze do standardní báze.
[30] Ano, je to děsivě komplikovaná formulace, ale musíme být přesní…
[31] Ověření linearity přenecháváme čtenáři jako minutkové zabavení.
[32] Tedy z definice maticového násobení.

Jak jistě každý střelhbitě zjistí, tato soustava nemá (pro libovolnou volbu parametrů $x_{i,j}$) řešení, tedy „matice zobrazení“ požadovaného typu vůbec ***neexistuje****! My to ale nevzdáme, situaci zachráníme přechodem od vektorů z $\mathbb{R}^{2,2}$ ke sloupečkům jejich souřadnic v nějaké bázi*[33]*, což jsou vlastně prvky $\mathbb{R}^{4,1}$.*

Odvodíme si obrazy vektorů standardní báze

$$e_{1,1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad e_{1,2} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad e_{2,1} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad e_{2,2} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

ve které každé matici $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ přísluší sloupec souřadnic $(a\ b\ c\ d)^T$.

Zřejmě platí

$$Ae_{1,1} = e_{1,1}, \quad Ae_{1,2} = e_{1,1} + e_{1,2}, \quad Ae_{2,1} = e_{2,1}, \quad Ae_{2,2} = e_{2,2}.$$

Hledanou matici zobrazení $\mathbb{A}$ sestavíme podobně, jako v příkladu výše, do jejích sloupců zapíšeme souřadnice obrazů bazických vektorů $Ae_{i,j}$, tedy

$$\mathbb{A} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Jelikož pro libovolné $x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2} \in \mathbb{R}$ platí

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_{1,1} \\ x_{1,2} \\ x_{2,1} \\ x_{2,2} \end{pmatrix} = \begin{pmatrix} x_{1,1} + x_{1,2} \\ x_{1,2} \\ x_{2,1} \\ x_{2,2} \end{pmatrix},$$

odvozená matice dělá přesně to, co má! Tedy, vynásobíme-li jí sloupec souřadnic jakékoli matice, dostaneme sloupec souřadnic[34] *jejího obrazu při zobrazení A.*

Zavedení matice zobrazení

Ačkoli jsme pojem *souřadnice vektoru v bázi* začali používat již v části 2.6, jediné zavedené značení se vlastně týkalo jen souřadnicových funkcionálů $x_i^\#$ (viz definice 2.67), o kterých například víme, že jsou samy lineárními zobrazeními (věta 2.72). Projde-li si čtenář předchozí motivační část a zhodnotí četnost použití slova *souřadnice* (spolu s neustálým zdůrazňováním, zda jde o řádek či o sloupec), jistě ocení následující zavedení nového značení.

Definice 5.23. *Nechť V_n je vektorový prostor dimenze $n \in \mathbb{N}$, buď $\mathcal{X} = (x_1, \dots, x_n)$ nějaká jeho báze s příslušnými souřadnicovými funkcionály $x_1^\#, \dots, x_n^\# \in \mathcal{L}(V_n, T)$.* ***Souřadnicemi vektoru*** *$z \in V_n$* ***v bázi*** *$\mathcal{X}$ nazveme uspořádanou ntici*

$$(z)_{\mathcal{X}} := (x_1^\#(z), \dots, x_n^\#(z)) \in T^n \text{[35]}.$$

[33] Pro jednoduchost v té standardní.

[34] Zde opět oboje ve standardní bázi.

[35] Na tuto *n*tici můžeme také nahlížet jako na **řádkový** vektor.

Sloupec souřadnic vektoru z ***v bázi*** $\mathcal{X}$ *pak značíme*

$$\lceil z \rceil_{\mathcal{X}} := \begin{pmatrix} x_1^{\#}(z) \\ \vdots \\ x_n^{\#}(z) \end{pmatrix} \in T^{n,1}\,.$$

S využitím nového značení tedy můžeme požadovanou vlastnost hledané matice $\mathbb{A}$ zobrazení $A \in \mathcal{L}(P_m, Q_n)$ v bázích $\mathcal{X}$ a $\mathcal{Y}$ formulovat stručně jako

$$\forall z \in P : \mathbb{A} \cdot \lceil z \rceil_{\mathcal{X}} = \lceil Az \rceil_{\mathcal{Y}}\,. \tag{5.1}$$

Místo abychom matici zobrazení rovnou definovali[36], zamyslíme se ještě, co pro ni z vlastnosti (5.1) vlastně plyne. Označme vektory standardní báze prostoru T^m zapsané do sloupců jako $\mathbb{e}_1 = (1\ 0\ \cdots\ 0)^T, \ldots, \mathbb{e}_m = (0\ \cdots\ 0\ 1)^T$,[37] pro libovolnou matici $\mathbb{A} \in T^{n,m}$ pak rovnou z definice maticového násobení platí

$$\forall j \in \hat{m} : \mathbb{A} \cdot \mathbb{e}_j = \mathbb{A}_{:j}\,, \tag{5.2}$$

tedy že násobením vektory standardní báze zprava dostáváme sloupce této matice[38] Připomeňme, že z věty 2.72 dále víme, že libovolná báze $\mathcal{X} = (x_1, \ldots, x_m)$ splňuje vlastnost $\forall i, j \in \hat{m} : x_i^{\#}(x_j) = \delta_{ij}$, z čehož vyplývá, že

$$\forall j \in \hat{m} : \lceil x_j \rceil_{\mathcal{X}} = \mathbb{e}_j\,. \tag{5.3}$$

Zkombinujeme-li[39] dohromady rovnosti (5.1), (5.2) a (5.3), dostaneme pro hledanou matici $\mathbb{A}$ rovnost

$$\forall j \in \hat{m} : \mathbb{A}_{:j} = \mathbb{A} \cdot \mathbb{e}_j = \mathbb{A} \cdot \lceil x_j \rceil_{\mathbb{X}} = \lceil Ax_j \rceil_{\mathcal{Y}}\,,$$

tedy že matice $\mathbb{A}$ musí mít rozměr $n \times m$ a především:

„$\mathbb{A}$ musí ve svých sloupcích obsahovat obrazy Ax_j vektorů z báze $\mathcal{X}$ zapsané svými souřadnicemi v bázi $\mathcal{Y}$.“

Takže už konečně víme, jak by se taková matice zobrazení měla asi definovat!

Definice 5.24. *Nechť $A \in \mathcal{L}(P_m, Q_n)$, buď $\mathcal{X} = (x_1, \ldots, x_m)$ a $\mathcal{Y} = (y_1, \ldots, y_n)$ báze P_m, respektive Q_n. Matici ${}^{\mathcal{X}}\!A^{\mathcal{Y}} \in T^{n,m}$, jejíž prvky definujeme*

$$\forall i \in \hat{n}, \forall j \in \hat{m} : {}^{\mathcal{X}}\!A^{\mathcal{Y}}_{ij} := y_i^{\#}(Ax_j),$$

*nazveme **maticí zobrazení** A **v bázích** $\mathcal{X}, \mathcal{Y}$ (nebo „z báze $\mathcal{X}$ do báze $\mathcal{Y}$“). Matici lineárního operátoru ${}^{\mathcal{X}}\!A^{\mathcal{X}}$ zkráceně označíme ${}^{\mathcal{X}}\!A := {}^{\mathcal{X}}\!A^{\mathcal{X}}$.*

[36] Uvádění explicitních definic „natvrdo“, bez předchozích vysvětlení, úvah či příkladů se totiž mezi studenty zdá být velice nepopulární...

[37] Toto značení už jsme dříve několikrát použili.

[38] Zvídavý čtenář nechť se sám zamyslí nad tím, co bychom dostali násobením matice prvky standardní báze zleva (a jakého rozměru by tyto vektory vlastně měly být)!

[39] S bonusovou znalostí faktu, že každé lineární zobrazení stačí definovat na vektorech nějaké báze.

Příklad 5.25. *Uvažujme zobrazení $A \in \mathcal{L}(\mathbb{R}^4, \mathbb{R}^3)$ definované předpisem*

$$A(z_1, z_2, z_3, z_4) = (4z_1 + z_2 + z_4, z_1 + z_2 + 2z_4, 2z_1 + 3z_2 + 2z_3)\,.$$

Jelikož platí [40]

$$\begin{aligned} A(1,0,0,0) &= (4,1,2)\,,\\ A(0,1,0,0) &= (1,1,3)\,,\\ A(0,0,1,0) &= (0,0,2)\,,\\ A(0,0,0,1) &= (1,2,0)\,, \end{aligned}$$

matici zobrazení A ve standardních bázích odvodíme snadno,

$$^{\mathcal{E}_4}A^{\mathcal{E}_3} = \begin{pmatrix} 4 & 1 & 0 & 1\\ 1 & 1 & 0 & 2\\ 2 & 3 & 2 & 0 \end{pmatrix}.$$

Navíc, jak vyplývá z našich motivačních úvah výše a jak si brzy korektně dokážeme, není rozhodně žádnou náhodou, že pro každý vektor $(z_1, z_2, z_3, z_4) \in \mathbb{R}^4$ platí

$$\begin{pmatrix} 4 & 1 & 0 & 1\\ 1 & 1 & 0 & 2\\ 2 & 3 & 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} z_1\\ z_2\\ z_3\\ z_4 \end{pmatrix} = \begin{pmatrix} 4z_1 + z_2 + z_4\\ z_1 + z_2 + 2z_4\\ 2z_1 + 3z_2 + 2z_3. \end{pmatrix}$$

Příklad 5.26. *Pro zobrazení $A \in \mathcal{L}(\mathbb{R}^4, \mathbb{R}^3)$ z příkladu 5.25 odvodíme matici v jiných než standardních bázích, $^{\mathcal{X}}A^{\mathcal{Y}}$, kde $\mathcal{X} = (x_1, x_2, x_3, x_4)$, $\mathcal{Y} = (y_1, y_2, y_3)$,*

$$x_1 = (2,1,0,0),\ x_2 = (0,2,1,0),\ x_3 = (0,0,2,1),\ x_4 = (1,0,0,2)$$

a

$$y_1 = (1,0,1),\ y_2 = (1,1,0),\ y_3 = (1,0,2).$$

Hledaná matice $^{\mathcal{X}}A^{\mathcal{Y}}$ má ve svých sloupcích obrazy Ax_i, zapsané svými souřadnicemi v bázi $\mathcal{Y}$. Nalezneme nejprve samotné obrazy. Protože $x_1 = 2e_1 + e_2$, máme

$$Ax_1 = 2Ae_1 + Ae_2 = 2(4,1,2) + (1,1,3) = (9,3,7).$$

Stejným způsobem spočítáme

$$Ax_2 = (2,2,8), \quad Ax_3 = (1,2,4), \quad Ax_4 = (6,5,2).$$

Nyní je třeba najít souřadnice těchto vektorů v bázi $\mathcal{Y}$, které nám vyjdou[41]

$$\begin{aligned} Ax_1 &= 5y_1 + 3y_2 + y_3,\\ Ax_2 &= -8y_1 + 2y_2 + 8y_3,\\ Ax_3 &= -6y_1 + 2y_2 + 5y_3,\\ Ax_4 &= 5y_2 + y_3. \end{aligned}$$

Odtud dostáváme

$$^{\mathcal{X}}A^{\mathcal{Y}} = \begin{pmatrix} 5 & -8 & -6 & 0\\ 3 & 2 & 2 & 5\\ 1 & 8 & 5 & 1 \end{pmatrix}.$$

---

[40] Jak snadno zjistíme dosazením

[41] Hledat souřadnice v bázi už samozřejmě dávno umíme.

Jak už víme z dřívějška, samotné souřadnicové funkcionály $x_i^\#$ jsou lineární zobrazení. Čistě tohoto faktu pak můžeme přímočaře využít a dokázat, že vlastně i takové přiřazení mezi zobrazením a jeho maticí, $A \to {}^{\mathcal{X}}A^{\mathcal{Y}}$, je lineární zobrazení. Připomeňme přitom, že i zobrazení můžeme mezi sebou sčítat, případně násobit zobrazení skalárem, konkrétně pro libovolná zobrazení $A, B \in \mathcal{L}(P, Q)$ a $\alpha \in T$ definujeme

$$\forall x \in P : (A + B)x := Ax + Bx\,, \quad (\alpha A)x := \alpha \cdot Ax\,.$$

Věta 5.27. *Nechť $A, B \in \mathcal{L}(P_m, Q_n)$, $\alpha \in T$. Potom platí*

(i) ${}^{\mathcal{X}}(A + B)^{\mathcal{Y}} = {}^{\mathcal{X}}A^{\mathcal{Y}} + {}^{\mathcal{X}}B^{\mathcal{Y}}$,

(ii) ${}^{\mathcal{X}}(\alpha A)^{\mathcal{Y}} = \alpha\, {}^{\mathcal{X}}A^{\mathcal{Y}}$.

Důkaz. Obě tvrzení vyplývají z linearity souřadnicových funkcionálů. Porovnáme ijté prvky příslušných matic, kde $i \in \hat{n}$ a $j \in \hat{m}$ jsou libovolné:

(i)

$$\begin{aligned}\left[{}^{\mathcal{X}}(A + B)^{\mathcal{Y}}\right]_{ij} &= y_i^\# \left((A + B)x_j\right) = y_i^\# \left(Ax_j + Bx_j\right) = y_i^\# \left(Ax_j\right) + y_i^\# \left(Bx_j\right) \\ &= \left[{}^{\mathcal{X}}A^{\mathcal{Y}}\right]_{ij} + \left[{}^{\mathcal{X}}B^{\mathcal{Y}}\right]_{ij}\end{aligned}$$

(ii)

$$\left[{}^{\mathcal{X}}(\alpha A)^{\mathcal{Y}}\right]_{ij} = y_i^\# \left((\alpha A)x_j\right) = y_i^\# \left(\alpha Ax_j\right) = \alpha y_i^\# \left(Ax_j\right) = \left[\alpha\, {}^{\mathcal{X}}A^{\mathcal{Y}}\right]_{ij}$$

□

Celé naše dosavadní úsilí směřovalo k jedné hlavní vlastnosti matice zobrazení, aby šlo jejím násobením ze souřadnic vzorů vyrábět souřadnice obrazů. I když se může zdát, že jsme si v motivačním úvodu důkaz této vlastnosti už vlastně odbyli, není to tak úplně pravda. Odvodili jsme si sice, co matice zobrazení **nutně musí** splňovat, ale kromě několika pozitivních příkladů[42] nám pořád zbývá dokázat, že tato podmínka k požadované vlastnosti **postačuje**.

Jinými slovy, oproti důkazu věty 3.14 provedeném na konci části 5.4, kde jsme k daným maticím definovali zobrazení a o těch něco dokazovali, zde postupujeme opačným směrem, dokazujeme různé vlastnosti matic, které podle jednoznačného předpisu přiřazujeme daným lineárním zobrazením.

Věta 5.28. *Nechť $A \in \mathcal{L}(P_m, Q_n)$, $\mathcal{X} = (x_1, \ldots, x_m)$ je báze P_m a $\mathcal{Y} = (y_1, \ldots, y_n)$ je báze Q_n.*

(i) Pro každé $z \in P_m$ platí

$$\lceil Az \rceil_{\mathcal{Y}} = {}^{\mathcal{X}}A^{\mathcal{Y}} \cdot \lceil z \rceil_{\mathcal{X}}\,,$$

[42] Nic jako „důkaz příkladem“ neexistuje! Pokud vám někdo někdy tvrdil opak, lhal a shoří v pekle. Pozor ale, vyvrátit nějaké tvrzení uvedením takzvaného *protipříkladu* je naprosto v pořádku a je třeba toto rozlišovat (vždycky je snazší bořit než budovat).

(ii) Pro každé $z \in P_m, w \in Q_n$ platí, že z je vzorem w (tedy $z \in A^{-1}w$, respektive $Az = w$) právě tehdy, když

$\lceil z \rceil_{\mathcal{X}}$ je řešením soustavy lineárních rovnic s rozšířenou maticí $\left({}^{\mathcal{X}}A^{\mathcal{Y}} \,\middle|\, \lceil w \rceil_{\mathcal{Y}} \right)$.

Důkaz. (i) Na obou stranách dokazované rovnosti jsou sloupcové vektory z $T^{n,1}$,[43] dokážeme tedy pro libovolné $i \in \hat{n}$ rovnost jejich $i$tých složek.

Začneme prachobyčejným rozepsáním pravé strany pomocí maticového násobení a následným dosazením, čemu se příslušné prvky v násobených maticích rovnají:

$$\begin{aligned} \left({}^{\mathcal{X}}A^{\mathcal{Y}} \cdot \lceil z \rceil_{\mathcal{X}} \right)_i &= \sum_{k=1}^{m} \left({}^{\mathcal{X}}A^{\mathcal{Y}} \right)_{ik} \cdot (\lceil z \rceil_{\mathcal{X}})_k \\ &= \sum_{k=1}^{m} y_i^{\#}(Ax_k) \cdot x_k^{\#}(z) \\ &= \sum_{k=1}^{m} \underbrace{x_k^{\#}(z)}_{\in T} \cdot y_i^{\#}(Ax_k)\,. \end{aligned}$$

Jelikož $y_i^{\#}$ je lineární funkcionál a na poslední sumu můžeme nahlížet jako na lineární kombinaci obrazů $y_i^{\#}(\cdots)$, využijeme tuto linearitu a dostáváme,

$$\left({}^{\mathcal{X}}A^{\mathcal{Y}} \cdot \lceil z \rceil_{\mathcal{X}} \right)_i = y_i^{\#} \left(\sum_{k=1}^{m} \underbrace{x_k^{\#}(z)}_{\in T} \cdot Ax_k \right),$$

kde v každém sčítanci sumy napravo opět vidíme lineární kombinaci obrazů, tentokráte pro lineární zobrazení A. Ještě jednou tedy sumu upravíme v duchu pozorování 5.5 (tedy „vytknutím“ lineárního zobrazení ze sumy ven) a pak už jen prozkoumáme, čemu se různé členy v sumě rovnají. Platí

$$\left({}^{\mathcal{X}}A^{\mathcal{Y}} \cdot \lceil z \rceil_{\mathcal{X}} \right)_i = y_i^{\#} \Bigg(A \underbrace{\left(\sum_{k=1}^{m} x_k^{\#}(z) \cdot x_k \right)}_{=z} \Bigg),$$

přičemž poslední krok jistě nikdo nepřekvapil, jde v něm o obyčejné rozepsání vektoru z pomocí souřadnic v bázi $\mathcal{X}$! Tedy platí

$$\forall i \in \hat{n} : \ \left({}^{\mathcal{X}}A^{\mathcal{Y}} \cdot \lceil z \rceil_{\mathcal{X}} \right)_i = y_i^{\#}(Az) = \left(\lceil Az \rceil_{\mathcal{Y}} \right)_i$$

a důkaz je hotov[44].

(ii) Každou maticovou rovnici ve tvaru $\mathbb{A} \cdot \mathbb{x} = \mathbb{b}$, kde $\mathbb{A} \in T^{n,m}$ je matice a $\mathbb{x} \in T^{m,1}, \mathbb{b} \in T^{n,1}$ jsou sloupcové vektory, lze chápat jako soustavu lineárních rovnic s rozšířenou maticí $(\mathbb{A} \mid \mathbb{b})$ a neznámými zapsanými do sloupce $\mathbb{x}$. Tvrzení pak přímo plyne z uvědomění si faktu, že $z \in P_m$ je vzorem $w \in Q_n$ právě tehdy když platí ${}^{\mathcal{X}}A^{\mathcal{Y}} \cdot \lceil z \rceil_{\mathcal{X}} = \lceil w \rceil_{\mathcal{Y}}$.

□

[43] Upřímně se nad tím zamyslete!

[44] Srdečné „Hurá!“ je jistě na místě.

Poznámka 5.29. *Věta 5.28 nám tedy říká:*

„Chceme-li najít obraz vektoru, musíme sloupec jeho souřadnic vynásobit maticí zobrazení. Chceme-li najít vzor vektoru, musíme vyřešit SLR s maticí soustavy rovnou matici zobrazení a pravou stranou rovnou sloupci souřadnic tohoto vektoru.“

Upozorněme ale, že k tomuto pravidlu ***nelze*** *přistupovat mechanicky a bez přemýšlení! V obou částech jsou totiž klíčové zvolené báze $\mathcal{X}$, $\mathcal{Y}$ a výsledek musíme vždy správně interpretovat jako souřadnice v dané bázi.*

Zobrazení samozřejmě umíme nejen sčítat nebo násobit číslem, lze je i skládat. To pro matice lineárního zobrazení nebude znamenat nic moc nového, vystačíme si s maticovým násobením. Jako příjemný důsledek nám pak přirozeně vyplyne pravidlo, podle kterého získáme matici inverzního zobrazení (pokud existuje) klasickou maticovou inverzí.

Věta 5.30. *Nechť $A \in \mathcal{L}(Q_n, V_s)$, $B \in \mathcal{L}(P_m, Q_n)$ a $\mathcal{X}, \mathcal{Y}, \mathcal{W}$ jsou popořadě báze P_m, Q_n, V_s. Potom pro matici složeného zobrazení $AB \in \mathcal{L}(P_m, V_s)$ platí*

$$^{\mathcal{X}}(AB)^{\mathcal{W}} = {}^{\mathcal{Y}}A^{\mathcal{W}} \cdot {}^{\mathcal{X}}B^{\mathcal{Y}}.$$

Důkaz. Nejprve si uvědomíme, že uvedený součin matic má smysl, neboť ${}^{\mathcal{Y}}A^{\mathcal{W}} \in T^{s,n}$, ${}^{\mathcal{X}}B^{\mathcal{Y}} \in T^{n,m}$, tedy ${}^{\mathcal{Y}}A^{\mathcal{W}} \cdot {}^{\mathcal{X}}B^{\mathcal{Y}} \in T^{s,m}$. Levá strana rovnice má také odpovídající rozměry ${}^{\mathcal{X}}(AB)^{\mathcal{W}} \in T^{s,m}$.

Pro prvek matice ${}^{\mathcal{X}}(AB)^{\mathcal{W}}$ s indexy $i \in \hat{s}$, $j \in \hat{m}$ platí[45]:

$$\begin{aligned}
{}^{\mathcal{X}}(AB)^{\mathcal{W}}_{ij} &= w_i^{\#}((AB)x_j) \\
&= w_i^{\#}(A(Bx_j)) \\
&= w_i^{\#}\left(A\left(\sum_{k=1}^{n} y_k^{\#}(Bx_j)y_k\right)\right) \\
&= w_i^{\#}\left(A\left(\sum_{k=1}^{n} {}^{\mathcal{X}}B^{\mathcal{Y}}_{kj}\, y_k\right)\right) \\
&= w_i^{\#}\left(\sum_{k=1}^{n} {}^{\mathcal{X}}B^{\mathcal{Y}}_{kj}\, Ay_k\right) \\
&= \sum_{k=1}^{n} {}^{\mathcal{X}}B^{\mathcal{Y}}_{kj}\, w_i^{\#}(Ay_k) \\
&= \sum_{k=1}^{n} {}^{\mathcal{X}}B^{\mathcal{Y}}_{kj}\, {}^{\mathcal{Y}}A^{\mathcal{W}}_{ik} \\
&= \sum_{k=1}^{n} {}^{\mathcal{Y}}A^{\mathcal{W}}_{ik}\, {}^{\mathcal{X}}B^{\mathcal{Y}}_{kj}\,,
\end{aligned}$$

což podle definice násobení matic dokazuje tvrzení věty. □

[45] Během úprav použijeme kromě definice příslušných matic a maticového násobení v podstatě jen dva „téměř-triky“: rozepsání vektoru pomocí souřadnic jako lineární kombinace prvků báze a oblíbený fakt, že lineární obraz lineární kombinace je lineární kombinace lineárních obrazů.

Důsledek 5.31. *Je-li $A \in \mathcal{L}(P_m, Q_n)$ izomorfismus (tedy $m = n$), potom je matice ${}^{\mathcal{X}}A^{\mathcal{Y}}$ regulární a platí*

$$\left({}^{\mathcal{X}}A^{\mathcal{Y}}\right)^{-1} = {}^{\mathcal{Y}}(A^{-1})^{\mathcal{X}}.$$

Důkaz. K bijektivnímu zobrazení $A \in \mathcal{L}(P_n, Q_n)$ vždy existuje zobrazení inverzní, které je také lineární a k němuž existuje matice v libovolných bázích. S využitím věty 5.30 pak platí

$${}^{\mathcal{X}}A^{\mathcal{Y}} \cdot {}^{\mathcal{Y}}(A^{-1})^{\mathcal{X}} = {}^{\mathcal{Y}}(AA^{-1})^{\mathcal{Y}} = {}^{\mathcal{Y}}E^{\mathcal{Y}} = \mathbb{E}\,,$$

kde poslední rovnost plyne z faktu, že vektory libovolné báze $\mathcal{Y} = (y_1, \ldots, y_n)$ splňují[46]

$$\forall i, j \in \hat{n} : y_i^{\#}(y_j) = \delta_{ij} \quad \Rightarrow \quad \forall j \in \hat{n} : \lceil y_j \rceil_{\mathcal{Y}} = \mathbb{e}_j \quad \Rightarrow \quad {}^{\mathcal{Y}}E^{\mathcal{Y}} = \mathbb{E}\,.$$

Z rovnosti

$${}^{\mathcal{X}}A^{\mathcal{Y}} \,.\, {}^{\mathcal{Y}}(A^{-1})^{\mathcal{X}} = \mathbb{E}$$

pak vyplývá tvrzení důsledku, matice na levé straně rovnosti jsou vůči sobě navzájem inverzemi. □

Na začátku části 5.4 jsme důsledně varovali před nahodilým zaměňováním pojmů *hodnost matice* a *hodnost zobrazení*. I když toto varování stále trvá, dokážeme si, že mezi oběma hodnostmi přece jen existuje souvislost. Zvolíme-li konkrétní báze vektorových prostorů P_m, Q_n, pak hodnost libovolného zobrazení $A \in \mathcal{L}(P_m, Q_n)$ bude rovna hodnosti jeho matice v těchto bázích.

Věta 5.32. *Nechť $A \in \mathcal{L}(P_m, Q_n)$, $\mathcal{X}$ je báze P_m a $\mathcal{Y}$ je báze Q_n. Potom platí*

$$h(A) = h({}^{\mathcal{X}}A^{\mathcal{Y}}).$$

Důkaz. Z definice hodnosti zobrazení a linearity odvodíme

$$h(A) = \dim AP_m = \dim A\langle x_1, \ldots, x_m\rangle = \dim\langle Ax_1, \ldots, Ax_m\rangle.$$

Jelikož souřadnicové izomorfismy $y_i^{\#}$ jsou lineárními zobrazeními, pak i přiřazení $z \to \lceil z \rceil_{\mathcal{Y}}$ je lineárním zobrazením (je to dokonce izomorfismus, jak plyne z našich dosavadních znalostí o souřadnicích v bázi!). Současně víme, že každé prosté lineární zobrazení zachovává jak lineární obal, tak lineární nezávislost (viz věta 5.7) a dokonce i dimenzi. Tedy v lineárním obalu výše můžeme jednotlivě vektory Ax_i nahradit jejich souřadnicemi $\lceil Ax_i \rceil_{\mathcal{Y}}$, aniž bychom změnili dimenzi jejich lineárního obalu[47] a dostáváme

$$\dim\langle Ax_1, \ldots, Ax_m\rangle = \dim\langle \lceil Ax_1 \rceil_{\mathcal{Y}}, \ldots, \lceil Ax_m \rceil_{\mathcal{Y}}\rangle.$$

Jenže vektory $\lceil Ax_1 \rceil_{\mathcal{Y}}, \ldots, \lceil Ax_m \rceil_{\mathcal{Y}}$ jsou přímo sloupce matice ${}^{\mathcal{X}}A^{\mathcal{Y}}$, a proto z vlastnosti hodnosti matice platí

$$h(A) = \dim\langle \lceil Ax_1 \rceil_{\mathcal{Y}}, \ldots, \lceil Ax_m \rceil_{\mathcal{Y}}\rangle = h({}^{\mathcal{X}}A^{\mathcal{Y}}).$$

□

[46] Jak se již stává milou tradicí, čtenář si jistě sám důkladně rozmyslí, proč následující implikace platí, případně si zopakuje významy použitých symbolů…

[47] Rozmyslí-li si čtenář sám přesnou posloupnost myšlenek, která k tomuto závěru vede, odměnou mu jistě bude hřejivý pocit porozumění.

Důsledek 5.33. *Zobrazení $A \in \mathcal{L}(P_m, Q_n)$ je izomorfismus, právě když je matice ${}^{\mathcal{X}}A^{\mathcal{Y}}$ regulární. V takovém případě nutně platí $m = n$.*

5.6 Změna báze

Jak jsme viděli např. v příkladech 5.10 a 5.26, práce se souřadnicemi vektorů v bázích není vždy triviální. Je totiž poměrně pracné přecházet mezi souřadnicemi v různých bázích u více zadaných vektorů (opakovaně řešíme podobné SLR), podobně pracné úvahy pak musíme provádět při odvození matice zobrazení v jiných bázích, než ve kterých je zadáno. Práci nám zjednoduší zavedení *matice přechodu*.

Definice 5.34. *Nechť $\mathcal{X} = (x_1, \ldots, x_n)$ a $\mathcal{Y} = (y_1, \ldots, y_n)$ jsou báze V_n. Matici identického operátoru ${}^{\mathcal{X}}E^{\mathcal{Y}} \in T^{n,n}$ nazýváme **maticí přechodu** od báze $\mathcal{X}$ k bázi $\mathcal{Y}$.*

Matice přechodu mezi bázemi $\mathcal{X}$ a $\mathcal{Y}$ tedy ve svých sloupcích obsahuje souřadnice vektorů z $\mathcal{X}$ vzhledem k bázi $\mathcal{Y}$. Jelikož se vlastně jedná jen o speciální případ matice lineárního zobrazení (pro volbu $A = E$), klíčové vlastnosti matic přechodu snadno odvodíme z již dokázaných tvrzení o maticích zobrazení.

Věta 5.35. *Nechť $\mathcal{X}$, $\mathcal{Y}$ a $\mathcal{Z}$ jsou báze V_n. Potom*

(i) matice ${}^{\mathcal{X}}E^{\mathcal{Y}}$ je regulární a platí

$$({}^{\mathcal{X}}E^{\mathcal{Y}})^{-1} = {}^{\mathcal{Y}}E^{\mathcal{X}},$$

(ii) pro libovolné $x \in V_n$ platí

$$({}^{\mathcal{X}}E^{\mathcal{Y}}) \cdot \lceil x \rceil_{\mathcal{X}} = \lceil x \rceil_{\mathcal{Y}},$$

(iii)

$${}^{\mathcal{Y}}E^{\mathcal{Z}} \cdot {}^{\mathcal{X}}E^{\mathcal{Y}} = {}^{\mathcal{X}}E^{\mathcal{Z}}.$$

Důkaz.

(i) Víme, že $h({}^{\mathcal{X}}A^{\mathcal{Y}}) = h(A)$ pro libovolné lineární zobrazení A. Identický operátor je bijekce, tedy platí $h(E) = n$ a matice ${}^{\mathcal{X}}E^{\mathcal{Y}}$ je regulární. Navíc je identický operátor sám sobě inverzí. Z důsledku 5.31 pak dostáváme

$$\left({}^{\mathcal{X}}E^{\mathcal{Y}}\right)^{-1} = {}^{\mathcal{Y}}(E^{-1})^{\mathcal{X}} = {}^{\mathcal{Y}}E^{\mathcal{X}}.$$

(ii) Vyplývá z věty 5.28.

(iii) Vyplývá z věty 5.30.

□

Poznámka 5.36. *Poznamenejme, že v různých materiálech k lineární algebře je možné objevit různé přístupy k přechodu z báze do báze! Někde se pojem matice přechodu vůbec nezavádí a pracuje se rovnou s identickým operátorem. Jinde (například v předchozích materiálech kurzu BI–LIN) se matice přechodu naopak zavádí se speciálním značením, namísto ${}^{\mathcal{X}}E^{\mathcal{Y}}$ například jako ${}_{\mathcal{X}}P_{\mathcal{Y}}$ nebo ${}_{\mathcal{Y}}P_{\mathcal{X}}$.*

Výpočet matice přechodu mezi dvěma obecnými bázemi (kdy ani jedna není standardní) si můžeme usnadnit, vzpomeneme-li si na hlavní myšlenku Algoritmu 3.19 pro hledání inverzních matic. Konkrétně na to, že při úpravách dvoublokové matice ve tvaru $(\mathbb{A} \mid \mathbb{B})$ pomocí GEM celou matici vlastně násobíme nějakou regulární maticí $\mathbb{P}$ a podaří-li se levý blok $\mathbb{A}$ vyeliminovat na matici jednotkovou, je příslušná matice úprav rovna $\mathbb{P} = \mathbb{A}^{-1}$, tedy

$$(\mathbb{A} \mid \mathbb{B}) \sim (\mathbb{P}\mathbb{A} \mid \mathbb{P}\mathbb{B}) \overset{\text{pro } \mathbb{A} \text{ reg.}}{\sim} (\mathbb{A}^{-1}\mathbb{A} \mid \mathbb{A}^{-1}\mathbb{B}) = (\mathbb{E} \mid \mathbb{A}^{-1}\mathbb{B})\,.$$

Algoritmus 5.37 (Sestrojení matice přechodu)**.** *Nechť $\mathcal{X}, \mathcal{Y}$ jsou dvě báze prostoru V_n. Sestavte matici přechodu ${}^{\mathcal{X}}E^{\mathcal{Y}}$.*

1. *Označme pomocí $\mathcal{E}$ standardní bázi V_n, případně jinou bázi, ve které umíme snadno hledat souřadnice vektorů.*

2. *Zapsáním souřadnic vektorů z $\mathcal{X}$ v bázi $\mathcal{E}$ popořadě do sloupců získáme rovnou matici přechodu ${}^{\mathcal{X}}E^{\mathcal{E}}$. Obdobně získáme matici ${}^{\mathcal{Y}}E^{\mathcal{E}}$.*

3. *Hledáme matici ${}^{\mathcal{X}}E^{\mathcal{Y}}$, pro kterou platí vztah*

$$\begin{aligned} {}^{\mathcal{X}}E^{\mathcal{Y}} &= {}^{\mathcal{E}}E^{\mathcal{Y}} \cdot {}^{\mathcal{X}}E^{\mathcal{E}} \\ &= ({}^{\mathcal{Y}}E^{\mathcal{E}})^{-1} \cdot {}^{\mathcal{X}}E^{\mathcal{E}}\,. \end{aligned}$$

4. *Hledaný součin nalezneme úpravou matice $({}^{\mathcal{Y}}E^{\mathcal{E}} \mid {}^{\mathcal{X}}E^{\mathcal{E}})$ pomocí GEM. Jelikož matice přechodu je vždy regulární, lze eliminací získat*

$$({}^{\mathcal{Y}}E^{\mathcal{E}} \mid {}^{\mathcal{X}}E^{\mathcal{E}}) \sim \left(\mathbb{E} \,\middle|\, ({}^{\mathcal{Y}}E^{\mathcal{E}})^{-1} \cdot {}^{\mathcal{X}}E^{\mathcal{E}}\right) = (\mathbb{E} \mid {}^{\mathcal{X}}E^{\mathcal{Y}})\,.$$

Příklad 5.38. *Uvažujme vektorový prostor $\mathbb{Z}_5^3$ s bázemi*

$$\mathcal{X} = ((1,0,1),(2,0,1),(3,1,0)) \qquad a \qquad \mathcal{Y} = ((0,1,1),(4,1,0),(2,1,0))\,,$$

sestrojíme matici přechodu ${}^{\mathcal{Y}}E^{\mathcal{X}}$.

Standardní bázi $\mathbb{Z}_5^3$ označme $\mathcal{E}$, snadno sestavíme matici přechodu z báze $\mathcal{X}$ (respektive $\mathcal{Y}$) do standardní báze:

$${}^{\mathcal{X}}E^{\mathcal{E}} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad {}^{\mathcal{Y}}E^{\mathcal{E}} = \begin{pmatrix} 0 & 4 & 2 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Podle algoritmu 5.37 sestavíme $({}^{\mathcal{X}}E^{\mathcal{E}} \mid {}^{\mathcal{Y}}E^{\mathcal{E}})$ a eliminujeme na $(\mathbb{E} \mid {}^{\mathcal{Y}}E^{\mathcal{X}})$: Dostaneme

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 0 & 4 & 2 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 4 & 1 \\ 0 & 1 & 0 & 1 & 1 & 4 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right).$$

Proto platí

$${}^{\mathcal{Y}}E^{\mathcal{X}} = \begin{pmatrix} 0 & 4 & 1 \\ 1 & 1 & 4 \\ 1 & 1 & 1 \end{pmatrix}.$$

Už jsme schopni sestavit matice přechodu mezi libovolnými bázemi, toho dále využijeme. Je-li potřeba ze znalosti matice lineárního zobrazení v zadaných bázích zkonstruovat jeho matici v bázích jiných, stačí si pořádně rozmyslet, v jakém pořadí matice zobrazení a matice přechodu „fungují“[48] a vhodným způsobem použít maticové násobení.

Hlavní větu této části nepotřebujeme nijak zvlášť dokazovat, je totiž přímým důsledkem věty 5.30 o matici složeného zobrazení[49].

Věta 5.39. *Nechť $A \in \mathcal{L}(P, Q)$, buď $\mathcal{X}$, $\tilde{\mathcal{X}}$ báze P a $\mathcal{Y}$, $\tilde{\mathcal{Y}}$ báze Q. Potom platí*

$$^{\tilde{\mathcal{X}}}A^{\tilde{\mathcal{Y}}} = {}^{\mathcal{Y}}E^{\tilde{\mathcal{Y}}} \cdot {}^{\mathcal{X}}A^{\mathcal{Y}} \cdot {}^{\tilde{\mathcal{X}}}E^{\mathcal{X}}.$$

Algoritmus 5.40 (Sestrojení matice zobrazení)**.** *Nechť $A \in \mathcal{L}(P, Q)$, $\mathcal{X}$ je báze P a $\mathcal{Y}$ je báze Q. Sestavte matici zobrazení ${}^{\mathcal{X}}A^{\mathcal{Y}}$.*

1. *Označme pomocí $\mathcal{E}$ standardní bázi prostoru Q, případně jinou bázi, ve které umíme snadno hledat souřadnice vektorů v Q.*

2. *Zapsáním souřadnic vektorů z $\mathcal{Y}$ v bázi $\mathcal{E}$ popořadě do sloupců získáme rovnou matici přechodu ${}^{\mathcal{Y}}E^{\mathcal{E}}$. Aplikujeme-li zobrazení A na vektory z báze $\mathcal{X}$ a souřadnice jejich obrazů v bázi $\mathcal{E}$ popořadě zapíšeme do sloupců, získáme matici zobrazení ${}^{\mathcal{X}}A^{\mathcal{E}}$.*

3. *Hledáme matici ${}^{\mathcal{X}}A^{\mathcal{Y}}$, pro kterou platí vztah*

$$\begin{aligned} {}^{\mathcal{X}}A^{\mathcal{Y}} &= {}^{\mathcal{E}}E^{\mathcal{Y}} \cdot {}^{\mathcal{X}}A^{\mathcal{E}} \\ &= ({}^{\mathcal{Y}}E^{\mathcal{E}})^{-1} \cdot {}^{\mathcal{X}}A^{\mathcal{E}} . \end{aligned}$$

4. *Hledaný součin nalezneme úpravou matice $({}^{\mathcal{Y}}E^{\mathcal{E}} \mid {}^{\mathcal{X}}A^{\mathcal{E}})$ pomocí GEM. Jelikož matice přechodu je vždy regulární, lze eliminací získat*

$$({}^{\mathcal{Y}}E^{\mathcal{E}} \mid {}^{\mathcal{X}}A^{\mathcal{E}}) \sim \left(\mathbb{E} \,\middle|\, ({}^{\mathcal{Y}}E^{\mathcal{E}})^{-1} \cdot {}^{\mathcal{X}}A^{\mathcal{E}}\right) = (\mathbb{E} \mid {}^{\mathcal{X}}A^{\mathcal{Y}}) .$$

Příklad 5.41. *Pro zobrazení $A \in \mathcal{L}(\mathbb{R}^4, \mathbb{R}^3)$ z příkladů 5.25 a 5.26 definované předpisem*

$$A(z_1, z_2, z_3, z_4) = (4z_1 + z_2 + z_4, z_1 + z_2 + 2z_4, 2z_1 + 3z_2 + 2z_3) .$$

odvodíme matici ${}^{\mathcal{X}}A^{\mathcal{Y}}$, kde $\mathcal{X} = (x_1, x_2, x_3, x_4)$, $\mathcal{Y} = (y_1, y_2, y_3)$,

$$x_1 = (2, 1, 0, 0),\ x_2 = (0, 2, 1, 0),\ x_3 = (0, 0, 2, 1),\ x_4 = (1, 0, 0, 2)$$

a

$$y_1 = (1, 0, 1),\ y_2 = (1, 1, 0),\ y_3 = (1, 0, 2) ,$$

[48] Každou matici zobrazení ${}^{\mathcal{X}}A^{\mathcal{Y}}$ si lze představit jako jakýsi stroj, který „na vstupu načte zprava souřadnice vektoru v levé bázi $\mathcal{X}$ a na výstupu pošle směrem doleva souřadnice obrazu tohoto vektoru v pravé bázi $\mathcal{Y}$“. Následuje-li vlevo další matice zobrazení, postup se opakuje. U matic přechodu je situace jednodušší, maticovým zobrazením se nekonstruuje žádný obraz vektoru, jen se mění použitá báze.

[49] Což samozřejmě neznamená, že se nad důkazem ani nezamyslíme, ba právě naopak!

a to s využitím matic přechodu. Můžeme v zásadě postupovat několika, velice podobnými, způsoby. Jednou z možností je začít odvozením matice zobrazení ve standardních bázích,

$$ {}^{\mathcal{E}_4}A^{\mathcal{E}_3} = \begin{pmatrix} 4 & 1 & 0 & 1 \\ 1 & 1 & 0 & 2 \\ 2 & 3 & 2 & 0 \end{pmatrix}, $$

a tu dále násobit vhodnými maticemi přechodu. Díky přímo zadaným bázím $\mathcal{X}$ a $\mathcal{Y}$ můžeme rovnou napsat matice přechodu ${}^{\mathcal{X}}E^{\mathcal{E}_4}$ a ${}^{\mathcal{Y}}E^{\mathcal{E}_3}$, dále pak platí

$$ \begin{aligned} {}^{\mathcal{X}}A^{\mathcal{Y}} &= ({}^{\mathcal{Y}}E^{\mathcal{E}_3})^{-1} \cdot {}^{\mathcal{E}_4}A^{\mathcal{E}_3} \cdot {}^{\mathcal{X}}E^{\mathcal{E}_4} \\ &= ({}^{\mathcal{Y}}E^{\mathcal{E}_3})^{-1} \cdot {}^{\mathcal{X}}A^{\mathcal{E}_3}. \end{aligned} $$

Po dosazení dostáváme

$$ {}^{\mathcal{X}}A^{\mathcal{Y}} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix}^{-1} \cdot \underbrace{\begin{pmatrix} 4 & 1 & 0 & 1 \\ 1 & 1 & 0 & 2 \\ 2 & 3 & 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 & 0 & 1 \\ 1 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 2 \end{pmatrix}}_{= {}^{\mathcal{X}}A^{\mathcal{E}_3}} $$

a díky asociativitě maticového násobení je v podstatě na nás, jak postupovat dále. Nic nám například nebrání postupně spočítat inverzi $({}^{\mathcal{Y}}E^{\mathcal{E}_3})^{-1}$ a pak postupně provést dvě maticová násobení. Případně nejdříve vynásobit poslední dvě matice, získat matici ${}^{\mathcal{X}}A^{\mathcal{E}_3}$ a na výsledek použít „trik“

$$ (\mathbb{A} \mid \mathbb{B}) \sim (\mathbb{E} \mid \mathbb{A}^{-1}\mathbb{B}). $$

Alternativně bychom mohli od začátku přesně následovat algoritmus 5.40, tedy nejprve odvodit obrazy vektorů z báze $\mathcal{X}$ a z jejich souřadnic v bázi $\mathcal{E}_3$ sestrojit jiným způsobem již výše zmíněnou matici ${}^{\mathcal{X}}A^{\mathcal{E}_3}$. Zbytek výpočtu by pak byl totožný s předchozím postupem [50].

Libovolným z uvedených postupů samozřejmě dostaneme hledanou matici,

$$ {}^{\mathcal{X}}A^{\mathcal{Y}} = \begin{pmatrix} 5 & -8 & -6 & 0 \\ 3 & 2 & 2 & 5 \\ 1 & 8 & 5 & 1 \end{pmatrix}. $$

5.7 Příklady lineárních zobrazení

Lineární zobrazení v rovině

V této části si spolu projdeme základní příklady lineárních operátorů na vektorovém prostoru $\mathbb{R}^2$ se standardní bází

$$ \mathcal{E} = (e_1, e_2) = ((1,0),(0,1)), $$

[50] Jak si čtenář jistě již domyslel, k valné části možných příkladů (nejen) na téma lineární zobrazení neexistuje jediný možný postup. O to důležitější je schopnost při řešení problémů **přemýšlet** a ne jen slepě kombinovat fragmenty nazpaměť naučených postupů! Správným pochopením tématu si navíc můžete výrazně ulehčit život; z více možných postupů lze při zapojení hlavy často vybrat nějaký „méně výpočetně náročný“, což každého jistě potěší.

které lze jednoduše geometricky interpretovat jako akce na bodech, případně orientovaných úsečkách v rovině (vycházejících z počátku). Jak už víme, každý lineární operátor $A \in \mathcal{L}(\mathbb{R}^2)$ můžeme jednoznačně charakterizovat maticí

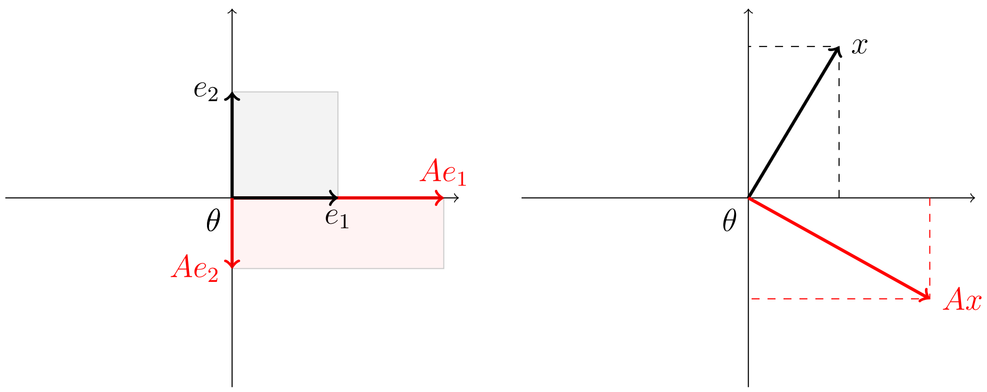
$$^{\mathcal{E}}A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} ,$$

pro kterou z definice platí[51]

$$^{\mathcal{E}}A = \left(\lceil Ae_1 \rceil_{\mathcal{E}} \; \lceil Ae_2 \rceil_{\mathcal{E}} \right) .$$

U všech typů operátorů níže si (více či méně jednoduše) právě matici ve standardní bázi $^{\mathcal{E}}A$ odvodíme. U všech příkladů si zobrazení znázorníme jednak obrazy prvků standardní báze (pro ilustraci doplněné obrazem „obdélníků“ s vrcholy $\theta, e_1, e_2, e_1+e_2$) a také obrazem obecného vektoru. V případech, kdy to bude potřeba, přejdeme i k bázi jiné než standardní.

Příklad 5.42 (Škálování ve směru os)**.** *Nechť $\alpha, \beta \in \mathbb{R}$, uvažujme lineární operátor, který „ve směru osy x“ násobí parametrem α a ve směru osy y násobí parametrem β.*



Obrázek 5.2: Operátor škálování podle os s parametry $\alpha = 2, \beta = -\frac{2}{3}$.

Zde snadno odvodíme hledanou matici přímo, každému vektoru v $\mathbb{R}^2$ zobrazení zřejmě přiřadí

$$(x_1, x_2) \xrightarrow{A} (\alpha x_1, \beta x_2) .$$

Obrazy jednotkových vektorů splňují

$$Ae_1 = \alpha e_1, Ae_2 = \beta e_2 ,$$

tedy platí

$$^{\mathcal{E}}A = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} .$$

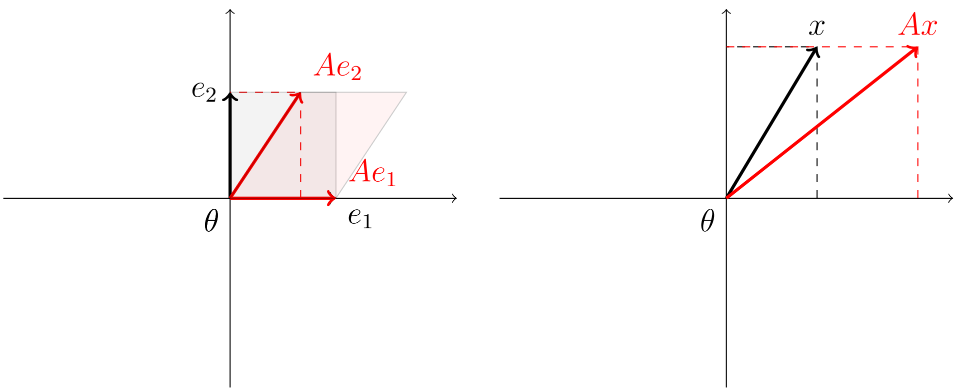
[51] Můžeme použít blokový zápis (po sloupcích).

Jak si čtenář jistě sám rozmyslí, v závislosti na konkrétních volbách $\alpha, \beta \in \mathbb{R}$ lze do škatulky *operátory škálování dle os* „schovat“ různá speciální zobrazení, jakými je například zrcadlení podle osy x (resp. y), projekce na osu x (resp. y) nebo středová symetrie podle počátku θ.

Jak lze snadno odvodit, zobrazení škálování je bijekcí právě tehdy, když platí $\alpha \neq 0$ a současně $\beta \neq 0$ a příslušné inverzní zobrazení má matici ve tvaru

$$^{\mathcal{E}}(A^{-1}) = \begin{pmatrix} \frac{1}{\alpha} & 0 \\ 0 & \frac{1}{\beta} \end{pmatrix} \text{[52]} .$$

Příklad 5.43 (Zkosení ve směru jedné z os)**.** *Nechť $\lambda \in \mathbb{R}$, uvažujme lineární operátor, který vektory ve směru osy y zachovává (nemění) a ve směru osy x je zvětšuje o λnásobek druhé složky. Jinými slovy, každý vektor je „zkosen“ ve směru osy x přímo úměrně své složce y.*



Obrázek 5.3: Operátor zkosení podle osy x s parametrem $\lambda = \frac{2}{3}$.

Hledanou matici opět odvodíme přímo, každému vektoru v $\mathbb{R}^2$ zobrazení přiřadí

$$(x_1, x_2) \xrightarrow{A} (x_1 + \lambda x_2, x_2) .$$

Obrazy jednotkových vektorů splňují

$$Ae_1 = e_1, Ae_2 = e_2 + \lambda e_1 ,$$

tedy platí

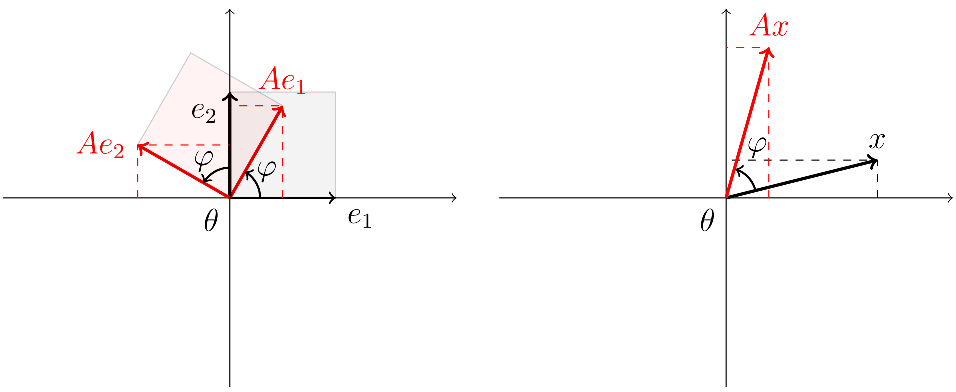
$$^{\mathcal{E}}A = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} .$$

Jak snadno poznáme z tvaru matice $^{\mathcal{E}}A$, zobrazení zkosení je vždy bijekce a příslušné inverzní zobrazení je také zkosením, jeho matice je

$$^{\mathcal{E}}(A^{-1}) = \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} .$$

[52]Toto lze odvodit dvěma způsoby! Buďto „maticově“, s využitím pravidla že matice inverzního zobrazení je inverzí původní matice, nebo „zobrazovací úvahou“, při které hledáme takové zobrazení, jehož aplikací na každý obraz při zobrazení A dostaneme původní vektor (tedy škálujeme „nazpátek“).

Příklad 5.44 (Rotace okolo počátku)**.** *Nechť $\varphi \in \mathbb{R}$, uvažujme lineární operátor, který vektory rotuje okolo počátku o úhel φ proti směru hodinových ručiček*[53]*.*



Obrázek 5.4: Operátor rotace o úhel φ s parametrem $\varphi = \frac{\pi}{3}$.

Zde je již odvození matice zobrazení o něco složitější. Nicméně, namísto obrazu obecného vektoru stačí odvodit obrazy prvků nějaké báze, nejlépe té standardní. K tomu nám může posloužit jednoduchá geometrická úvaha (jejíž podrobné promyšlení ponecháváme na čtenáři[54]*), která vede k poznání, že platí*

$$A(1,0) = (\cos\varphi, \sin\varphi)\,, \quad A(0,1) = (-\sin\varphi, \cos\varphi)\,,$$

z čehož přímo odvozujeme

$$^{\mathcal{E}}A = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}\,.$$

Takže, jak plyne z rovnice $\lceil Ax \rceil_{\mathcal{E}} = {}^{\mathcal{E}}A \cdot \lceil x \rceil_{\mathcal{E}}$, pro obecný vektor platí

$$(x_1, x_2) \xrightarrow{A} (x_1 \cos\varphi - x_2 \sin\varphi, x_1 \sin\varphi + x_2 \cos\varphi)\,.$$

Pro odvození matice inverzního zobrazení můžeme klasicky invertovat matici $^{\mathcal{E}}A$, musíme při tom ale dávat pozor na korektnost prováděných kroků GEM[55]*! Alternativní postup spočívá v úvaze, že složíme-li zobrazení rotující o φ se zobrazením rotujícím o stejný úhel v opačném směru $-\varphi$, dostaneme zobrazení identické. Tedy příslušná skládaná zobrazení jsou sobě navzájem inverzní. Jelikož pro každé $\varphi \in \mathbb{R}$ platí $\cos(-\varphi) = \cos\varphi$ a $\sin(-\varphi) = -\sin\varphi$, dostáváme vztah*

$$^{\mathcal{E}}(A^{-1}) = \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix}^{56}\,.$$

[53] Jde tedy o přímé zobecnění motivačního příkladu z úvodu části 5.5, kde jsme vektory rotovali o úhel $\varphi = \frac{\pi}{2}$.

[54] Stačí ve znázornění obecného bodu v rovině nalézt vhodný pravoúhlý trojúhelník a zavzpomínat na vlastnosti funkcí sinus a kosinus.

[55] Provádění více kroků najednou v duchu „od $\sin\varphi$násobku jednoho řádku odečtu $\cos\varphi$násobek druhého“ nemusí být korektní a musíme zvažovat různé podmínky pro nenulovost skalárů, jimiž násobíme. Podmínkami vyloučené případy pak musíme ošetřit zvlášť

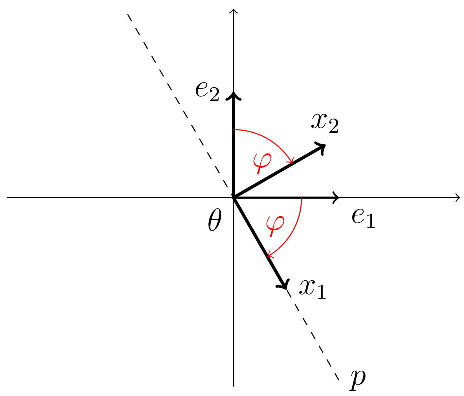
[56] No a jelikož z žádného našeho kroku nevyplynula žádná podmínka na úhel φ, operátor rotace je vždy bijekcí.

Následující příklady lineárních operátorů budou o něco složitější, k jejich jednoduchému popisu už nebudou stačit pouze osy x a y, důležitou roli bude hrát i daná obecná přímka[57] p procházející počátkem. I když by nejspíš bylo možné odvodit matice mnohých z následujících zobrazení čistě geometrickou úvahou, existuje snadnější způsob, a to s využitím matice přechodu. Klíčovým krokem je nalezení jiné báze než standardní, a to takové, ve které lze dané zobrazení popsat mnohem jednodušeji. Převod do standardní báze lze pak provést klasickým způsobem, podle věty 5.39.

Lze například zvolit bázi $\mathcal{X} = (x_1, x_2)$ tak, aby vektor x_1 ležel v zaměření příslušné přímky p a vektor x_2 byl na něj kolmý (opět v tradičním geometrickém smyslu, jak známe „ze školy“), to lze udělat například tak, že vezmeme standardní bázi a aplikujeme na ní rotaci o úhel φ. S využitím příkladu 5.44 odvodíme, že vektory této nové báze splňují

$$\mathcal{X} = (x_1, x_2) = \Big((\cos\varphi, \sin\varphi), (-\sin\varphi, \cos\varphi)\Big)\,. \tag{5.4}$$

Navíc, jak čtenář jistojistě sám odhalí, není náhodou[58], že matice přechodu ${}^{\mathcal{X}}E^{\mathcal{E}}$ je rovna matici rotace o úhel φ ve standardní bázi.

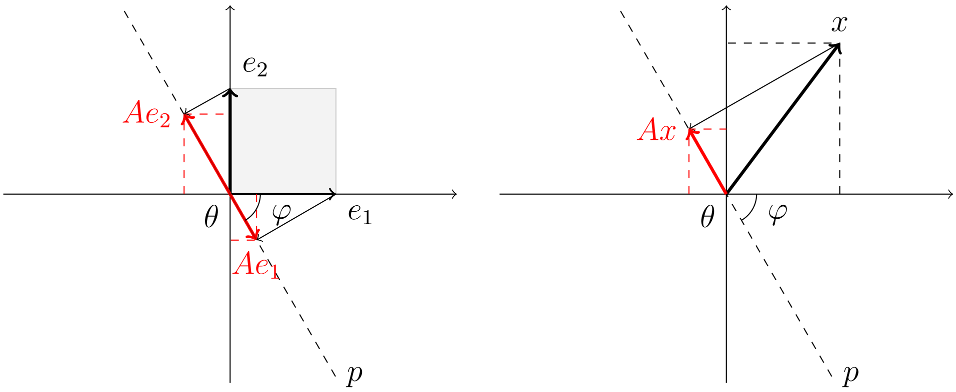


Příklad 5.45 (Projekce na přímku)**.** *Nechť $\varphi \in \mathbb{R}$ a p je přímka procházející počátkem, která svírá s osou x úhel φ. Uvažujme lineární operátor, který každému vektoru v $\mathbb{R}^2$ přiřadí kolmým promítnutím na přímku p bod na této přímce*[59].

[57] Při dostatku odvahy možná i dvě obecné přímky...

[58] V lineární algebře žádné náhody nemáme.

[59] Pojmu „kolmý“ zde rozumíme jaksi naivně, v souladu s tím co známe z hodin klasické rovinné geometrie. Klasikové by snad lépe porozuměli popisu „Z vektoru $x \in \mathbb{R}^2$ spustíme kolmici na přímku p a bod u paty této kolmice pak bude obrazem bodu x.“



Obrázek 5.5: Operátor projekce na přímku svírající úhel φ s osou x, s parametrem $\varphi = -\frac{\pi}{3}$.

Ač se mnohému čtenáři jistě nabízí možnost využít svých hlubokých znalostí pravoúhlých trojúhelníků a s nimi souvisejících geometrických znalostí k odvození obrazů vektorů standardní báze $\mathcal{E} = (e_1, e_2)$, my zde alibisticky přejdeme ke „zrotované“ bázi $\mathcal{X}$ zavedené v (5.4) s vektorem x_1 ležícím v zaměření přímky p a vektorem x_2 na ni kolmým. Sestavení matice projekce v bázi $\mathcal{X} = (x_1, x_2)$ je totiž triviální, neboť jistě platí $Ax_1 = x_1$ a $Ax_2 = \theta$ a tedy

$$^{\mathcal{X}}A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} .$$

Se znalostí báze $\mathcal{X}$ sestavíme příslušné matice přechodu a hledanou matici $^{\mathcal{E}}A$ odvodíme dle věty 5.39:

$$\begin{aligned} ^{\mathcal{E}}A &= {}^{\mathcal{X}}E^{\mathcal{E}} \cdot {}^{\mathcal{X}}A \cdot {}^{\mathcal{E}}E^{\mathcal{X}} \\ &= {}^{\mathcal{X}}E^{\mathcal{E}} \cdot {}^{\mathcal{X}}A \cdot ({}^{\mathcal{X}}E^{\mathcal{E}})^{-1} \\ &= \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \\ &= \begin{pmatrix} \cos^2\varphi & \sin\varphi\cos\varphi \\ \sin\varphi\cos\varphi & \sin^2\varphi \end{pmatrix} \end{aligned}$$

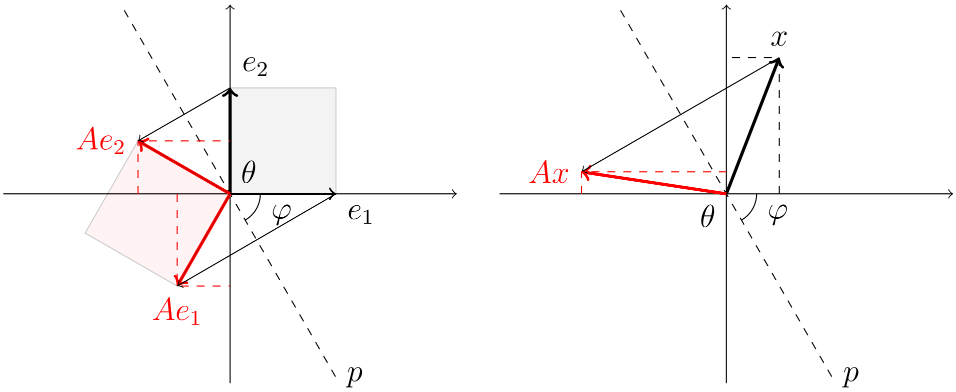
a, jelikož se jedná o singulární matici (soubor řádků je vždy LZ), projekce na přímku není nikdy bijekce[60].

Na závěr ještě podotkněme, že získanou matici lze ještě upravit do (pro někoho možná esteticky líbivějšího) tvaru

$$^{\mathcal{E}}A = \begin{pmatrix} \frac{1+\cos(2\varphi)}{2} & \frac{\sin(2\varphi)}{2} \\ \frac{\sin(2\varphi)}{2} & \frac{1-\cos(2\varphi)}{2} \end{pmatrix}$$

[60] Což bychom ostatně mohli odvodit i jednoduchou úvahou o (ne)injektivitě tohoto zobrazení, například odvozením jádra ker A!.

Příklad 5.46 (Zrcadlení podle přímky)**.** *Nechť $\varphi \in \mathbb{R}$ a p je přímka procházející počátkem, která svírá s osou x úhel φ. Uvažujme lineární operátor, který každému vektoru v $\mathbb{R}^2$ přiřadí vektor osově souměrný podle přímky p.*



Obrázek 5.6: Operátor zrcadlení podle přímky svírající úhel φ s osou x, s parametrem $\varphi = -\frac{\pi}{3}$.

Podobně jako v příkladu 5.45, namísto geometrického odvozování přejdeme pro jednoduchost k bázi $\mathcal{X}$ zavedené v (5.4) s vektorem x_1 ležícím v zaměření přímky p a vektorem x_2 na ni kolmým. Matici zrcadlení v bázi $\mathcal{X} = (x_1, x_2)$ odvodíme ze zřejmých vztahů $Ax_1 = x_1$ a $Ax_2 = -x_2$ jako

$$^{\mathcal{X}}A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} .$$

Se znalostí báze $\mathcal{X}$ sestavíme příslušné matice přechodu a hledanou matici $^{\mathcal{E}}A$ odvodíme dle věty 5.39:

$$\begin{aligned} ^{\mathcal{E}}A &= {}^{\mathcal{X}}E^{\mathcal{E}} \cdot {}^{\mathcal{X}}A \cdot {}^{\mathcal{E}}E^{\mathcal{X}} \\ &= {}^{\mathcal{X}}E^{\mathcal{E}} \cdot {}^{\mathcal{X}}A \cdot ({}^{\mathcal{X}}E^{\mathcal{E}})^{-1} \\ &= \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \\ &= \begin{pmatrix} \cos^2\varphi - \sin^2\varphi & 2\sin\varphi\cos\varphi \\ 2\sin\varphi\cos\varphi & \sin^2\varphi - \cos^2\varphi \end{pmatrix} , \end{aligned}$$

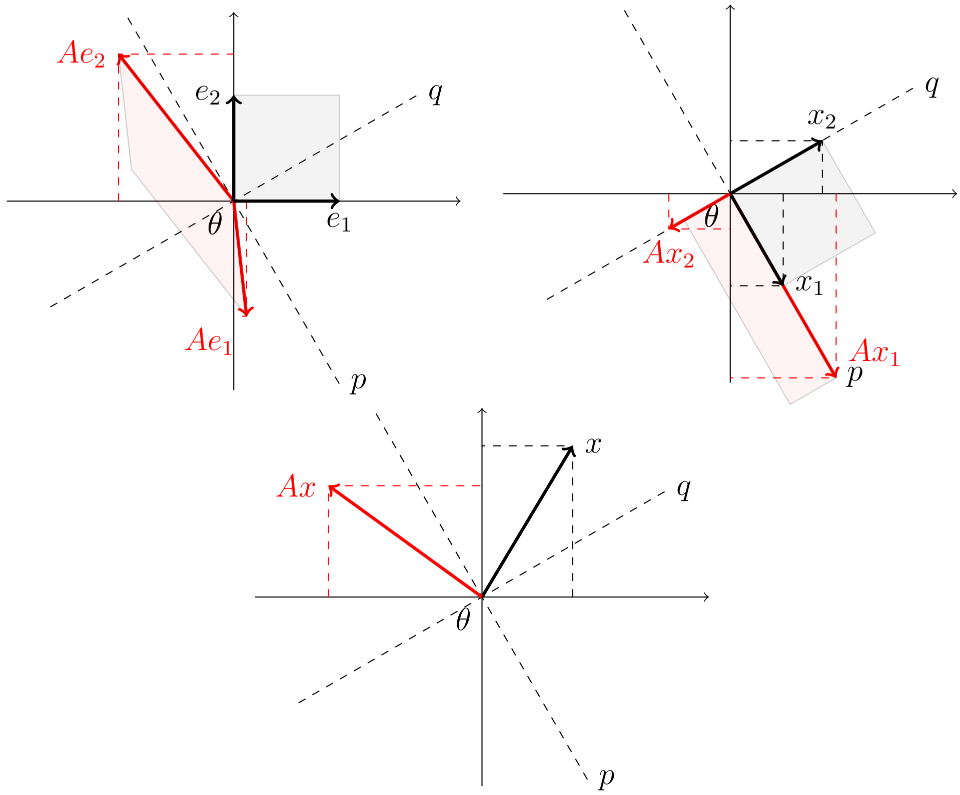
což pomocí známých vzorců rovnou upravíme na

$$^{\mathcal{E}}A = \begin{pmatrix} \cos(2\varphi) & \sin(2\varphi) \\ \sin(2\varphi) & -\cos(2\varphi) \end{pmatrix} .$$

Na závěr se ještě zamysleme nad regularitou matice $^{\mathcal{E}}A$, respektive nad tím, zda je A bijekce, či ne. Ať už k tomu dospějeme libovolnou úvahou[61]*, můžeme konstatovat, že zrcadlení podle přímky je vždy bijekce a je dokonce samo sobě zobrazením inverzním, tedy $A = A^{-1}$.*

[61] Nalezením inverzní matice, zjištěním že platí $\ker A = \{\theta\}$, nebo uvědoměním si, že aplikací zobrazení zrcadlení dvakrát za sebou na libovolný vektor dostaneme tentýž vektor…

Příklad 5.47 (Obecnější škálování podle přímek). *Nechť $\varphi \in \mathbb{R}$ a p je přímka procházející počátkem, která svírá s osou x úhel φ. Uvažujme lineární operátor, který ve směru přímky p násobí parametrem α a ve směru kolmém na ni (přímka q) násobí parametrem β.*



Obrázek 5.7: Operátor škálování podle os otočených o úhel φ s parametry $\alpha = 2, \beta = -\frac{1}{2}, \varphi = -\frac{\pi}{3}$.

Podobně jako v příkladech výše přejdeme pro jednoduchost k bázi $\mathcal{X}$ s vektorem x_1 ležícím v zaměření přímky p a vektorem x_2 na ni kolmým. Matici zobrazení v bázi $\mathcal{X} = (x_1, x_2)$ odvodíme ze zřejmých vztahů $Ax_1 = \alpha x_1$ a $Ax_2 = \beta x_2$ jako

$$^{\mathcal{X}}A = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}.$$

Se znalostí báze $\mathcal{X}$ sestavíme příslušné matice přechodu a hledanou matici $^{\mathcal{E}}A$ odvodíme dle věty 5.39:

$$\begin{aligned}
^{\mathcal{E}}A &= {}^{\mathcal{X}}E^{\mathcal{E}} \cdot {}^{\mathcal{X}}A \cdot {}^{\mathcal{E}}E^{\mathcal{X}} \\
&= {}^{\mathcal{X}}E^{\mathcal{E}} \cdot {}^{\mathcal{X}}A \cdot ({}^{\mathcal{X}}E^{\mathcal{E}})^{-1} \\
&= \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \cdot \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \cdot \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \\
&= \begin{pmatrix} \alpha\cos^2\varphi + \beta\sin^2\varphi & (\alpha - \beta)\sin\varphi\cos\varphi \\ (\alpha - \beta)\sin\varphi\cos\varphi & \alpha\sin^2\varphi + \beta\cos^2\varphi \end{pmatrix}.
\end{aligned}$$

Jelikož víme, že hodnost zobrazení se rovná hodnosti jeho matice v libovolných bázích, můžeme o bijektivitě zobrazení A rozhodnout například z matice ${}^{\mathcal{X}}A$, tedy dostaneme podmínku, že škálování podél otočených os je bijekce právě tehdy, když $\alpha \neq 0$ a současně $\beta \neq 0$ (nezávisle na úhlu otočení φ). Nalezení matice inverzního zobrazení ponecháváme na čtenáři a jeho svobodné úvaze.

Příklad 5.48 (Ještě obecnější škálování)**.** *Pro nadměrně zvídavého čtenáře můžeme škálovací zobrazení zobecnit ještě dále. Nechť $\varphi, \psi \in \mathbb{R}$ a uvažujme zobrazení, které ve směru přímky p (zadané úhlem φ, který svírá s osou x) násobí vektory parametrem $\alpha \in \mathbb{R}$ a ve směru další přímky q (která s osou x svírá úhel ψ) násobí parametrem $\beta \in \mathbb{R}$.*

Aby bylo zobrazení dobře definováno, musí jistě platit, aby byly obě uvažované přímky různé, tedy aby $\varphi - \psi \notin \{k\pi \mid k \in \mathbb{Z}\}$. Poznamenejme, že na příklad 5.47 pak můžeme nahlížet jako na speciální případ s volbou $\psi = \varphi + \frac{\pi}{2}$.

Odvození matice tohoto zobrazení ve standardní matice nebudeme provádět až do konce[62], alespoň nastíníme základní možný postup.

I zde lze najít vhodnou bázi, označme ji jako $\mathcal{Y}$, jejíž vektory leží jeden ve směru přímky p a druhý ve směru přímky q. Zvolíme jako vektor y_1 obraz bazického vektoru e_1 při otočení o úhel φ, podobně y_2 zvolíme jako obraz e_1 při otočení o úhel ψ. Snadno pak odvodíme matici přechodu

$$
{}^{\mathcal{Y}}E^{\mathcal{E}} = \begin{pmatrix} \cos\varphi & \cos\psi \\ \sin\varphi & \sin\psi \end{pmatrix} {}^{63}
$$

a podobně snadno bychom odvodili i matici zobrazení A v této bázi $\mathcal{Y}$. Matici ve standardní bázi bychom pak získali tradičním postupem,

$$
\begin{aligned}
{}^{\mathcal{E}}A &= {}^{\mathcal{Y}}E^{\mathcal{E}} \cdot {}^{\mathcal{Y}}A \cdot {}^{\mathcal{E}}E^{\mathcal{Y}} \\
&= {}^{\mathcal{Y}}E^{\mathcal{E}} \cdot {}^{\mathcal{X}}A \cdot ({}^{\mathcal{Y}}E^{\mathcal{E}})^{-1} \\
&= \begin{pmatrix} \cos\varphi & \cos\psi \\ \sin\varphi & \sin\psi \end{pmatrix} \cdot \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \cdot \begin{pmatrix} \cos\varphi & \cos\psi \\ \sin\varphi & \sin\psi \end{pmatrix}^{-1} .
\end{aligned}
$$

O rovnicích typu $Ax = b$

Jak si v této kraťounké závěrečné části k tématu o lineárních zobrazeních naznačíme, lineární algebra má značný přesah do mnoha dalších odvětví (nejen) matematiky. Nemálo problémů lze totiž formulovat následujícím způsobem:

Problém 5.49. *Nechť P, Q jsou libovolné vektorové prostory nad tělesem T a nechť je zadáno $A \in \mathcal{L}(P, Q)$ a $b \in Q$. Určete vzor $A^{-1}b$, tedy vyřešte rovnici*

$$
Ax = b\,.
$$

Množina řešení takové rovnice má pro libovolné volby prostorů i lineárního zobrazení vždy „podobný“ tvar, který by nám měl nápadně připomínat něco, co už známe – množinu řešení SLR.

[62] V zájmu zachování alespoň malé míry tajemství. . .

[63] Přičemž o tom, jak obecně vypadá matice k ní inverzní, pomlčíme.

Věta 5.50. *Nechť* $A \in \mathcal{L}(P,Q)$, $b \in Q$. *Existuje-li vektor* $\tilde{x} \in P$ *splňující* $A\tilde{x} = b$, *pak platí*
$$A^{-1}b = \tilde{x} + \ker A\,.$$

Důkaz. Dokážeme, že pro každé $x \in P$ platí ekvivalence $x \in A^{-1}b \Leftrightarrow x \in \tilde{x} + \ker A$. Nechť tedy $x \in P$, pak platí

$$\begin{aligned} x \in A^{-1}b &\Leftrightarrow Ax = b \\ &\Leftrightarrow Ax = A\tilde{x} \\ &\Leftrightarrow A(x - \tilde{x}) = \theta_Q \\ &\Leftrightarrow x - \tilde{x} \in \ker A \\ &\Leftrightarrow \exists z \in \ker A : x - \tilde{x} = z \\ &\Leftrightarrow \exists z \in \ker A : x = \tilde{x} + z \\ &\Leftrightarrow x \in \tilde{x} + \ker A\,. \end{aligned}$$

□

Tedy množina všech řešení rovnic typu $Ax = b$ je buď prázdná nebo je *lineární varietou v prostoru* P, což je přirozené zobecnění pojmu, který už známe, z prostorů T^n do prostorů obecných[64].

Další poznatek, který se týká jádra zobrazení A, už máme také k dispozici, jedná se o *2. větu o dimenzi* (v textu věta 5.14), kterou zde zopakujeme.

Věta 5.51. *Nechť* $A \in \mathcal{L}(P,Q)$. *Potom*

$$h(A) + d(A) = \dim P.$$

Tedy kromě toho, že množina všech řešení rovnice $Ax = b$ je lineární varieta se zaměřením $\ker A$, navíc víme, že dimenze této variety není nic jiného než $\dim \ker A$, tedy defekt zobrazení A. Ten pak lze v některých případech z 2. věty o dimenzi dopočítat[65].

Projdeme si několik základních typů rovnic tvaru $Ax = b$.

Soustavy lineárních rovnic

Předpokládejme, že $P = T^m$ a $Q = T^n$ pro nějaké těleso T a $m, n \geq 1$[66]. Pak pro každé $A \in \mathcal{L}(P,Q) = \mathcal{L}(T^m, T^n)$ existuje matice $\mathbb{A} \in T^{n,m}$ taková, že pro každý vektor $\mathbb{x} \in T^m$ platí $A\mathbb{x} = \mathbb{A} \cdot \mathbb{x}$ (tato matice $\mathbb{A}$ je rovna matici ve standardních bázích $\mathbb{A} = {}^{\mathcal{E}_m}A^{\mathcal{E}_n}$).

Pro danou volbu vektorových prostorů je tedy rovnice $Ax = b$ pouhou soustavou lineárních rovnic! Navíc platí:

[64] Žádná velká věda, lineární varietou je libovolná množina ve tvaru „vektor plus podprostor", ať už v jakémkoli vektorovém prostoru

[65] V případech, kdy je alespoň jedno z čísel $h(A)$ a $\dim P$ konečné, aby mělo smysl je od sebe odečítat.

[66] Vskutku šokující volba…

- Množina řešení přidružené homogenní soustavy $A\mathbb{x} = \mathbb{A} \cdot \mathbb{x} = \theta$ je rovna přímo jádru $\ker A$. Tedy první část Frobeniovy věty 3.24 je pouhým důsledkem věty 5.50, pro vyřešení SLR je potřeba a stačí vyřešit přidruženou homogenní soustavu rovnic a k jejímu řešení přičíst jakékoli partikulární řešení celé soustavy i s pravou stranou.

- Jelikož $h(A) = h(\mathbb{A})$, $\dim P = \dim T^m = m$ a pro množinu řešení přidružené homogenní soustavy platí $S_0 = \ker A$, plyne druhá část Frobeniovy věty 3.24 přímo z 2. věty o dimenzi,

$$h(A) + d(A) = \dim P \quad \Rightarrow \quad h(\mathbb{A}) + \dim S_0 = m \quad \Rightarrow \quad \dim S_0 = m - h(\mathbb{A})\,.$$

Lineární rekurentní rovnice

Předpokládejme, že $P = Q = T^\infty$ pro nějaké těleso T. Kromě identického operátoru E patří mezi základní typy lineárních operátorů *operátor posunutí* $S \in \mathcal{L}(T^\infty)$[67] definovaný předpisem

$$x = (x_1, x_2, x_3, \dots) \;\Rightarrow\; Sx := (x_2, x_3, x_4, \dots)\,,$$

případně kompaktněji jako

$$\forall x \in T^\infty, \forall n \in \mathbb{N}: \;(Sx)_n := x_{n+1}\,.$$

K operátoru S lze pochopitelně definovat jeho mocniny, tedy složení S vícekrát samo se sebou, což je vždy také lineární operátor a zjevně platí[68]

$$\forall k \in \mathbb{N}, \forall n \in \mathbb{N}: (S^k x)_n = x_{n+k}\,.$$

Jelikož platí, že součet lineárních operátorů a skalární násobek lineárního operátoru je také lineární operátor, můžeme se spolu s klidným svědomím omezit na takové operátory $A \in \mathcal{L}(T^\infty)$, které jsou lineárními kombinacemi operátorů $E, S, S^2, \dots$. Například operátor $A = S^2 - S^1 - E$ je definován předpisem

$$\forall n \in \mathbb{N}: \;A(x_1, x_2, x_3, \dots) := (x_3 - x_2 - x_1, x_4 - x_3 - x_2, x_5 - x_4 - x_3, \dots)$$

a pro zajímavost uveďme, že například taková Fibonacciho posloupnost[69] je jedním z mnoha řešení rovnice $Ax = \theta$ pro operátor $A = S^2 - S - E$.

Lineární rekurentní rovnice s konstantními koeficienty je pak libovolná rovnice typu $Ax = b$, kde $b \in T^\infty$ je pevně zvolená posloupnost a lineární operátor $A \in \mathcal{L}(T^\infty)$ je libovolnou lineární kombinací $A = \sum_{k=0}^{n} \alpha_k S^k$ kde $\alpha_0, \dots, \alpha_k \in T$ a formálně značíme $S^0 = E$.

Rovnici $Ax = b$ pak zapisujeme ve tvaru

$$\forall n \in \mathbb{N}: \;\alpha_k x_{n+k} + \alpha_{k-1} x_{n+k-1} + \dots + \alpha_1 x_{n+1} + \alpha_0 x_n = b_n\,.$$

[67] S jako posunutí, tedy shift.

[68] Ctihodný čtenář si již jistě stačil zvyknout na to, že výrazy jako *zjevně* nebo *triviálně* jsou diplomatickou zkratkou pro „čtenář si sám dokáže“.

[69] $(1, 1, 2, 3, 5, 8, 13, 21, \dots)$

Příklad 5.52. *Pro ilustraci vyřešíme lineární rekurentní rovnici*

$$\forall n \in \mathbb{N}: \; x_{n+1} - 2x_n = 1 - n\,,$$

v prostoru $\mathbb{R}^\infty$. Z teorie vyplývá, že je třeba najít všechna řešení přidružené homogenní rovnice (výsledkem musí být podprostor) a jedno řešení celé rekurentní rovnice.

- *Přidruženou homogenní rovnici $x_{n+1} - 2x_n = 0$ pro každé $n \in \mathbb{N}$ lze vyřešit snadno, jejími řešeními jsou zjevně všechny geometrické posloupnosti s kvocientem 2, tedy $x_n = \alpha \cdot 2^n$ pro libovolné $\alpha \in \mathbb{R}$. Jinými slovy,* $\ker A = \langle (2^n)_{n\geq 1} \rangle$.
- *Pravou stranou rovnice je posloupnost $(1-n)_{n\geq 1} = (0, -1, -2, \dots)$ a poměrně snadno lze uhádnout*[70]*, že partikulárním řešením rovnice $\forall n \in \mathbb{N} : x_{n+1} - 2x_n = 1 - n$ je například posloupnost $\tilde{x}$ splňující $\tilde{x}_n = n$.*
- *Každé řešení zadané rekurence tedy leží v množině $(n)_{n\geq 1} + \langle (2^n)_{n\geq 1} \rangle$, což většinou zapisujeme jako*

$$x_n = n + \alpha \cdot 2^n \text{ pro nějaké } \alpha \in \mathbb{R}\,.$$

Lineární diferenciální rovnice

Předpokládejme, že $P = Q = \mathcal{F}$ je vektorový prostor všech hladkých[71] reálných funkcí reálné proměnné (tedy $T = \mathbb{R}$). Podobně jako u rekurentních rovnic si lze i zde zavést několik jednoduchých lineárních operátorů a pak se omezit na rovnice $Ax = b$, kde $A \in \mathcal{L}(\mathcal{F})$ je jejich lineárních kombinací.

- Identický operátor můžeme honosněji označit jako $E = D^0$.
- Dále zavedeme operátor derivování D, který každé funkci $f \in \mathcal{F}$ přiřadí její derivaci, $\forall f \in \mathcal{F} : Df := f'$.
- Operátor $D \in \mathcal{L}(\mathcal{F})$ lze samozřejmě mocnit a platí, že D^k přiřadí každé funkci její $k$tou derivaci.
- *Lineární diferenciální rovnicí s konstantními koeficienty* pak nazveme libovolnou rovnici $Ax = b$, kde $b \in \mathcal{F}$ je pevně zvolená funkce a operátor $A \in \mathcal{L}(\mathcal{F})$ je lineární kombinací operátorů $D^k, k \in \mathbb{N}_0$.

Příklad 5.53. *Vyřešíme*[72] *lineární diferenciální rovnici*

$$\forall x \in \mathbb{R}: \; f(x) - f'(x) = 42$$

(tedy $f \xrightarrow{A} f - f'$). Z teorie vyplývá, že je třeba najít všechna řešení přidružené homogenní rovnice (výsledkem musí být podprostor) a jedno partikulární řešení celé rovnice.

[70] Na detaily ohledně tohoto hádání a preciznější postupy zde nemáme prostor. Jsou však stálou náplní kurzu BI-ZDM, Základů diskrétní matematiky.

[71] Hladká funkce je taková která je nejen spojitá, ale navíc k ní existují derivace všech řádů a ty jsou také spojité.

[72] Nicméně velmi ilustračním a neformálním způsobem.

- *Přidruženou homogenní rovnici* $f(x) - f'(x) = 0$ *pro každé* $x \in \mathbb{R}$ *řeší všechny funkce, které se rovnají svým vlastním derivacím. To že mezi ně patří všechny exponenciální funkce* $\alpha \cdot e^x$*, kde* $\alpha \in \mathbb{R}$*, jistě víme z BI–ZMA. Tomu, že žádné jiné funkce z* $\mathcal{F}$ *už tuto vlastnosti nesplňují, zde můžeme skromně věřit. Platí tedy* $\ker A = \langle e^x \rangle$.

- *Pravou stranou rovnice je konstantní funkce splňující* $\forall x \in \mathbb{R} : b(x) = 42$. *Snadno uhádneme*[73]*, že jedním z řešení celé rovnice* $f(x) - f'(x) = 42$ *je tatáž konstantní funkce* $\tilde{f}(x) = 42$.

- *Každé řešení zadané rovnice tedy leží v množině* $42 + \langle e^x \rangle$*, což většinou zapisujeme jako*
$$f(x) = 42 + \alpha \cdot e^x \text{ pro nějaké } \alpha \in \mathbb{R}\,.$$

[73]Díky tomu, že derivace konstantní funkce je všude nulová.

Kapitola 6

Determinant matice

V této kapitole budeme pracovat pouze v tělese racionálních, reálných nebo komplexních čísel. Kdykoliv zde tedy mluvíme o tělese T, máme na mysli $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$.

Nejprve se v motivační části kapitoly (podkapitola 6.2) pokusíme čtenáře přivést k determinantu pomocí studia nutné a postačující podmínky pro jednoznačnou řešitelnost soustav dvou (resp. tří) rovnic o dvou (resp. třech) neznámých. Následně v podkapitole 6.3 učiníme drobnou odbočku a zavedeme a studujeme pojem permutace, který dále využijeme při zavedení determinantu v podkapitole 6.4. Nakonec podrobně probereme vlastnosti tohoto nového pojmu v podkapitole 6.5 a ukážeme si různé metody jeho výpočtu v podkapitole 6.6.

6.1 Co si z této kapitoly odneseme

1. Seznámíme se s pojmy permutace množiny a determinantu matice.
2. Vysvětlíme si význam determinantu matice a probereme jeho vlastnosti.
3. Ukážeme si několik metod výpočtu determinantu matice.

6.2 Motivace

Pojďme se na začátku této kapitoly nejprve pokusit nastínit co determinant matice „determinuje“, tj. česky „určuje“. K formální definici (Definice č. 6.14) se dostaneme až v podkapitole 6.4.

Jednou z možných motivací (ne jedinou!) zavedení determinantu matice je snaha nalézt kritérium *jednoznačné řešitelnosti* soustavy

$$\mathbb{A}\mathbb{x} = \mathbb{b} \tag{6.1}$$

s *čtvercovou* maticí $\mathbb{A} \in \mathbb{R}^{n,n}$, resp. $\mathbb{C}^{n,n}$.

Rozeberme tuto otázku na soustavách dvou rovnic o dvou neznámých a tří rovnic o třech neznámých. Musíme zjistit, za jaké podmínky jsme schopni matici uvedené soustavy převést pomocí GEM na horního stupňovitý tvar nemající žádné vedlejší sloupce (vyjma sloupce pravých stran, ten ale v této úvaze nehraje roli a proto se mu nebudeme věnovat).

Případ matice 2×2

Uvažme nejprve pro jednoduchost úlohu (6.1) s maticí

$$\mathbb{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{R}^{2,2}.$$

Pokud $a = c = 0$ pak naše soustava má nekonečně mnoho řešení nebo žádné. Bez újmy na obecnosti dále předpokládejme, že $a \neq 0$ (jinak prohodíme řádky matice). Díky nenulovosti a je následující úprava ekvivalentní: druhý řádek soustavy nahraďme a násobkem druhého řádku od kterého odečteme c násobek prvního řádku, konkrétně

$$\mathbb{A} \sim \begin{pmatrix} a & b \\ 0 & ad - cb \end{pmatrix}.$$

Všimněme si, že pokud $a = c = 0$ pak i $ad - cb = 0$.

Můžeme proto učinit následující závěr o množině řešení soustavy (6.1) s maticí $\mathbb{A}$ uvedenou výše:

- pokud $ad - cb = 0$, pak má soustava (6.1) nekonečně mnoho nebo žádné řešení,
- pokud $ad - cb \neq 0$, pak má soustava (6.1) právě jedno řešení.

Hodnota (číslo) $ad - cb$ proto v tomto případě rozhoduje o jednoznačné řešitelnosti naší soustavy, determinuje ji. Tato hodnota bude v budoucnu to, co budeme nazývat determinantem takovéto 2×2 matice $\mathbb{A}$.

Případ matice 3×3

Budeme schopni předchozí výpočet zobecnit i pro matice 3×3? Vezměme opět soustavu (6.1) s maticí

$$\mathbb{A} = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & j \end{pmatrix} \in \mathbb{R}^{3,3}.$$

Je-li opět $a = d = g = 0$, pak má tato soustava nekonečně mnoho řešení nebo žádná. Bez újmy na obecnosti předpokládejme, že $a \neq 0$. Proveďme opět následující ekvivalentní úpravu (2 kroky stejné jako v předchozím případě matice 2×2):

- druhý řádek vynásobme číslem a a odečtěme od něj první řádek vynásobený číslem d,
- třetí řádek vynásobme číslem a a odečtěme od něj první řádek vynásobený číslem g.

Dostáváme tak ekvivalentní úpravu

$$\mathbb{A} = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & j \end{pmatrix} \sim \begin{pmatrix} a & b & c \\ 0 & ae - bd & af - cd \\ 0 & ah - bg & aj - cg \end{pmatrix}.$$

Soustřeďme se nyní nad „podsoustavu“ s 2×2 maticí v pravém dolním rohu. Z předchozího textu víme, že tato soustava bude mít právě jedno řešení, právě tehdy když platí

$$\begin{aligned}&(ae - bd)(aj - cg) - (ah - bg)(af - cd) = \\ &= a^2ej - aecg - bdaj + bdcg - a^2hf + ahcd + bgaf - bgcd = \\ &= a(aej - ecg - bdj - ahf + hcd + bgf)\end{aligned}$$

Vzhledem k předpokladu nenulovosti a dostáváme opět kritérium řešitelnosti soustavy (6.1) s 3×3 maticí uvedenou výše:

- pokud $aej + hcd + bgf - ecg - bdj - ahf = 0$, pak má soustava (6.1) nekonečně mnoho nebo žádné řešení,
- pokud $aej + hcd + bgf - ecg - bdj - ahf \neq 0$, pak má soustava (6.1) právě jedno řešení.

Tento pozoruhodný výraz (součet součinů prvků matice soustavy) opět rozhoduje o jednoznačné řešitelnosti dané soustavy. Lze takto pokračovat i v případě lineárních soustav n rovnic o n neznámých? Na tuto otázku čtenáři kladně odpovíme v následujících odstavcích.

Závěrečná motivace a poznámky

V předchozím textu jsme si ve speciálních případech reálných matic 2×2 a 3×3 našli podmínky pro řešitelnost soustavy $\mathbb{A}\mathbb{x} = \mathbb{b}$.

Vnímavý čtenář mezi oběma případy vidí jistou souvislost. Nejprve u matice soustavy

$$\mathbb{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{R}^{2,2}$$

byl rozhodujícím výrazem výraz

$$ad - bc. \tag{6.2}$$

Ten je tvořen rozdílem součinů dvou prvků matice $\mathbb{A}$. Ovšem ne všech možných! Všimněte si, že členy v součtu jsou jediné dva součiny, které lze z prvků matice $\mathbb{A}$ vybrat tak, aby neležely ve stejném řádku ani sloupci.

Podobně v případě matice soustavy

$$\mathbb{A} = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & j \end{pmatrix} \in \mathbb{R}^{3,3}$$

byl rozhodujícím výrazem výraz

$$aej + hcd + bgf - ecg - bdj - ahf. \tag{6.3}$$

Opět jde o členy (případně vynásobené -1, zatím nevíme proč) jediných součinů trojic prvků matice $\mathbb{A}$ vybratelných tak, aby se při výběru neopakoval řádek ani sloupec.

Než se pustíme do samotné definice determinantu musíme udělat drobnou odbočku k permutacím. Pomocí nich totiž budeme teprve schopni přehledně popsat jak prvky z matice vybíráme a kdy zvolit znaménko + a kdy −.

6.3 Permutace

Význam latinského slovíčka *permutatio* je „změna“, „proměna“ nebo „výměna“. Čtenáře jistě nepřekvapí, že nejlepším způsobem jak popsat změnu (množiny) je pomocí zobrazení této množiny na sebe sama. My se budeme zabývat[1] permutacemi množiny $\hat{n} = \{1, 2, \ldots, n\}$, $n \in \mathbb{N}$. Formální definice zní následovně.

Definice 6.1. *Buď $n \in \mathbb{N}$. Každé zobrazení $\pi : \hat{n} \to \hat{n}$, které je bijekcí, nazýváme* ***permutací množiny*** *$\hat{n}$. Množinu všech permutací množiny $\hat{n}$ značíme symbolem S_n.*

Množina $\hat{n}$ má n prvků a proto existuje $n!$ různých permutací takovéto množiny. Množina S_n má tudíž $n!$ prvků. Permutace budeme značit malými řeckými písmenky jako[2] π, σ a τ.

Příklad 6.2. *Příkladem permutace množiny $\hat{3}$ by tedy mohlo být zobrazení $\pi : \hat{3} \to \hat{3}$ definované vztahy*

$$\pi(1) := 3, \ \pi(2) := 2, \ \pi(3) := 1.$$

Zjednodušený zápis permutací

Je očividné, že výše použitý způsob zadání permutace pomocí vypsání funkčních hodnot v každém bodě svého definičního oboru, tj. $\hat{n}$, není úplně nejefektivnější. Pro větší než menší n bude zápis poměrně nepřehledný.

K zjednodušení notace budeme proto využívat následující zápis permutace $\pi \in S_n$ pomocí uspořádané $n$tice jejích *funkčních* hodnot:

$$\pi = (\pi(1), \pi(2), \ldots, \pi(n)).$$

Tento zápis je podstatně kompaktnější. Permutaci π z Příkladu č. 6.2 nyní ekvivalentně můžeme zapsat následovně

$$\pi = (3, 2, 1). \tag{6.4}$$

Stále ale mějme na paměti, že permutace je *zobrazení* a zápis v rovnici (6.4) je jen zjednodušení notace. Permutace *není* $n$tice čísel.

Poznámka 6.3. *Způsob zápisu permutací pomocí uspořádané ntice je jednoduchý, ale není jediný možný a asi ani nejpoužívanější. V literatuře a v různých implementacích permutací můžete navíc narazit na tzv. cyklovou notaci. Té se zde nebudeme věnovat.*

Skládání a invertování permutací

Každá permutace $\pi \in S_n$ zobrazuje $\hat{n}$ na $\hat{n}$ a proto dvě takové permutace $\pi, \sigma \in S_n$ lze složit jakožto zobrazení. Např. pro permutace

$$\pi = (3, 1, 5, 2, 4) \quad \text{a} \quad \sigma = (1, 5, 4, 3, 2)$$

[1] To není žádné velké omezení. Každou konečnou množinu si lze takto očíslovat.

[2] Výslovnost pro našince nepolíbené řečtinou: *pí*, *sigma* a *tau*.

platí

$$\pi \circ \sigma = (3,4,2,5,1) \quad \text{a} \quad \sigma \circ \pi = (4,1,2,5,3).$$

Skutečně, spočtěme například $(\pi \circ \sigma)(2) = \pi(\sigma(2))$. σ zobrazí 2 na 5 a tuto hodnotu pak π zobrazí na 4. Podobně si můžeme napočítat další funkční hodnoty $\pi \circ \sigma$, resp. $\sigma \circ \pi$.

Jelikož je permutace bijekce množiny $\hat{n}$ na sebe samu, je její inverze také bijekce, a tedy permutace. Pro permutace uvedené výše platí

$$\pi^{-1} = (2,4,1,5,3) \quad \text{a} \quad \sigma^{-1} = (1,5,4,3,2).$$

Jak jsme na tyto výsledky přišli? Očividně v π^{-1} je $k \in \hat{n}$ na pozici $\ell \in \hat{n}$, právě když $\ell \in \hat{n}$ je na pozici $k \in \hat{n}$ v π. Jinak řečeno $\pi(k) = \ell$, právě když $\pi^{-1}(\ell) = k$.

Označíme-li si jako $e \in S_n$ permutaci $e = (1,2,\ldots,n)$, tj. permutaci odpovídající identickému zobrazení na $\hat{n}$, pak pro každou permutaci $\pi \in S_n$ přímo z definice platí

$$\pi \circ \pi^{-1} = e \quad \text{a} \quad \pi^{-1} \circ \pi = e. \tag{6.5}$$

Poznámka 6.4. *Množina všech permutací z S_n spolu s operací skládání tvoří grupu. Podrobněji binární operace $\circ$ na S_n splňuje asociativní zákon, existuje vůči ní neutrální prvek e a každý prvek $\pi \in S_n$ má inverzi π^{-1} splňující (6.5).*

Následující tvrzení několikrát využijeme při ověřování vlastností determinantu.

Tvrzení 6.5. *Buď π permutace z S_n. Definujme zobrazení $P : S_n \to S_n$ předpisem*

$$P(\sigma) := \pi \circ \sigma.$$

Potom je P bijekce.

Důkaz. Zobrazení P je surjektivní: máme-li libovolnou $\sigma \in S_n$ pak[3]

$$P(\pi^{-1} \circ \sigma) = \pi \circ (\pi^{-1} \circ \sigma) = (\pi \circ \pi^{-1}) \circ \sigma = \sigma.$$

Zobrazení P je injektivní: máme-li $\sigma_1, \sigma_2 \in S_n$ splňující $P(\sigma_1) = P(\sigma_2)$, pak

$$\pi \circ \sigma_1 = \pi \circ \sigma_2$$

a opět díky asociativitě skládání zobrazení konečně

$$\sigma_1 = (\pi^{-1} \circ \pi) \circ \sigma_1 = \pi^{-1} \circ (\pi \circ \sigma_1) = \pi^{-1} \circ (\pi \circ \sigma_2) = (\pi^{-1} \circ \pi) \circ \sigma_2 = \sigma_2. \qquad \square$$

Analogické tvrzení platí samozřejmě i pro zobrazení P definované předpisem $P(\sigma) := \sigma \circ \pi$. Důsledkem je, že máme-li jistou pevně zadanou permutaci $\pi \in S_n$ a libovolnou funkci $f : S_n \to \mathbb{R}$, pak platí

$$\sum_{\sigma \in S_n} f(\sigma) = \sum_{\sigma \in S_n} f(\pi \circ \sigma) = \sum_{\sigma \in S_n} f(\sigma \circ \pi). \tag{6.6}$$

Jediným rozdílem mezi uvedenými sumami je, že sčítáme v jiném (permutovaném) pořadí.

[3] Skládání zobrazení je asociativní!

Inverze v permutaci a znaménko permutace

Nyní zaveďme důležitý pojem inverze v permutaci, který úzce souvisí se znaménky ve vzorci pro determinant. V úvodní motivaci, konkrétně rovnice (6.2) a (6.3), u sebe některé členy měly $-$, jiné $+$. Důvod zatím nebyl zřejmý.

Definice 6.6. *Nechť $\pi \in S_n$. Každou dvojici $(\pi(i), \pi(j))$ takovou, že $i, j \in \hat{n}$ a*

$$i < j \quad a \quad \pi(i) > \pi(j)$$

nazýváme ***inverzí v permutaci*** *π. Číslo $(-1)^{I_\pi}$, kde I_π je počet inverzí v π, nazýváme* ***znaménko (signum)*** *permutace π, značíme $\operatorname{sgn} \pi$.*

Poznámka 6.7. *Pozor! Je důležité rozlišovat* inverzi permutace *(nová permutace) a* inverzi v permutaci *(jisté konstatování o dané permutaci). Vyzýváme poctivého čtenáře aby si sám slovně zkusil vysvětlit jaký je mezi těmito pojmy rozdíl.*

Příklad 6.8. *V permutaci $\pi = (3, 1, 5, 2, 4) \in S_5$ existují 4 inverze $(3, 1)$, $(3, 2)$, $(5, 2)$, $(5, 4)$: za číslem 3 se vyskytují menší čísla 1 a 2 a za číslem 5 se vyskytují menší čísla 2 a 4. Platí tedy, že $\operatorname{sgn} \pi = (-1)^4 = 1$. Identická permutace $e = (1, 2, 3, 4, 5) \in S_5$ žádnou inverzi neobsahuje proto $\operatorname{sgn} e = (-1)^0 = 1$.*

Transpozice

Nyní zmíníme speciální jednoduchý druhu permutací. Permutace, které odpovídají prohození právě dvou prvků v množině $\hat{n}$, budeme nazývat transpozice.

Definice 6.9. *Nechť $n \in \mathbb{N}$ a $i, j \in \hat{n}$, $i \neq j$. Permutaci $\tau_{ij} \in S_n$, kde*

1. *$\tau_{ij}(j) = i$,*
2. *$\tau_{ij}(i) = j$,*
3. *$\tau_{ij}(k) = k$, pro $k \neq i, j$,*

nazýváme ***transpozicí*** *čísel i a j.*

Příklad 6.10. *Například pro $\tau_{13} \in S_5$ platí $\tau_{13} = (3, 2, 1, 4, 5)$. Tato permutace zachovává pořadí prvků $2, 4, 5$, ale prohodí 1 a 3. Každá transpozice obsahuje lichý počet inverzí a proto má znaménko -1, $\operatorname{sgn} \tau_{ij} = -1$.*

Znaménko při skládání permutací

Na závěr této části textu si uvedeme důležitou větu o znaménku permutace a skládání permutací. Využijeme ji dále v textu.

Věta 6.11. *Nechť $\pi, \sigma \in S_n$, potom platí:*

$$\operatorname{sgn}(\pi \circ \sigma) = \operatorname{sgn} \pi \cdot \operatorname{sgn} \sigma.$$

Speciálně: složíme-li nějakou permutaci π s transpozicí τ, změní se znaménko:

$$\operatorname{sgn}(\pi \circ \tau) = \operatorname{sgn}(\tau \circ \pi) = -\operatorname{sgn} \pi.$$

Důkaz. První část důkazu spočívá v šikovném, početním, vyjádření znaménka permutace. Pro každou permutaci $\pi \in S_n$ platí

$$\operatorname{sgn} \pi = \prod_{i<j} \frac{\pi(j) - \pi(i)}{j - i}. \tag{6.7}$$

Zde velký symbol $\prod_{i<j}$ označuje součin uvedených výrazů přes všechny indexy $i, j \in \hat{n}$ splňující $i < j$. Opravdu, stačí si uvědomit, že všechny čitatele a jmenovatele ve výsledném zlomku lze pokrátit, a ty odpovídající inverzím v π se pokrátí na -1. Po této úpravě vidíme, že součin (6.7) představuje pouze součin tolika -1 kolik je inverzí v permutaci π. To je přesně definice znaménka permutace.

Nyní je důkaz relativně snadný, pro dvě permutace $\pi, \sigma \in S_n$ platí následující úvaha

$$\begin{aligned}
\operatorname{sgn}(\pi \circ \sigma) &= \prod_{i<j} \frac{\pi(\sigma(j)) - \pi(\sigma(i))}{j - i} = \prod_{i<j} \frac{\pi(\sigma(j)) - \pi(\sigma(i))}{\sigma(j) - \sigma(i)} \cdot \frac{\sigma(j) - \sigma(i)}{j - i} \\
&= \prod_{i<j} \frac{\pi(\sigma(j)) - \pi(\sigma(i))}{\sigma(j) - \sigma(i)} \cdot \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i} \\
&= \prod_{i<j} \frac{\pi(j) - \pi(i)}{j - i} \cdot \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i} \\
&= \operatorname{sgn}(\pi) \cdot \operatorname{sgn}(\sigma).
\end{aligned}$$

V první a poslední rovnosti jsme využili formulky (6.7). Druhá a třetí rovnost představuje jen vynásobení vhodně zvolenou jedničkou a využívá asociativity a komutativity násobení reálných čísel. Konečně ve čtvrté rovnosti jsme využili faktu, že množiny

$$\{\{i, j\} \mid i, j \in \hat{n},\ i < j\} \quad \text{a} \quad \{\{\sigma(i), \sigma(j)\} \mid i, j \in \hat{n},\ i < j\}$$

jsou totožné a oba příslušné produkty dávají stejnou hodnotu. □

Poznámka 6.12. *Pro větší názornost demonstrujme vzorec (6.7) na konkrétním příkladě permutace $\pi = (4, 3, 1, 2) \in S_4$. V této permutaci je celkem 5 inverzí a její znaménko je proto -1. Dosazení do (6.7) nám dává*

$$\begin{aligned}
&\prod_{i<j} \frac{\pi(j) - \pi(i)}{j - i} = \\
&= \frac{\pi(2) - \pi(1)}{2 - 1} \cdot \frac{\pi(3) - \pi(1)}{3 - 1} \cdot \frac{\pi(4) - \pi(1)}{4 - 1} \cdot \frac{\pi(3) - \pi(2)}{3 - 2} \cdot \frac{\pi(4) - \pi(2)}{4 - 2} \cdot \frac{\pi(4) - \pi(3)}{4 - 3} \\
&= \frac{3 - 4}{2 - 1} \cdot \frac{1 - 4}{3 - 1} \cdot \frac{2 - 4}{4 - 1} \cdot \frac{1 - 3}{3 - 2} \cdot \frac{2 - 3}{4 - 2} \cdot \frac{2 - 1}{4 - 3} = \frac{-1}{1} \cdot \frac{-3}{2} \cdot \frac{-2}{3} \cdot \frac{-2}{1} \cdot \frac{-1}{2} \cdot \frac{1}{1} = -1.
\end{aligned}$$

Důležitým a na první pohled netriviálním důsledkem Věty č. 6.11 je shodnost znaménka permutace a její inverze.

Důsledek 6.13. *Znaménka permutace a její inverze jsou stejná. Tj. pro libovolné $\pi \in S_n$ platí*

$$\operatorname{sgn} \pi = \operatorname{sgn} \pi^{-1}.$$

Důkaz. Protože $\pi \circ \pi^{-1} = e$, pak nutně dle Věty č. 6.11 platí $\operatorname{sgn}(\pi) \cdot \operatorname{sgn}(\pi^{-1}) = \operatorname{sgn} e = 1$. Znaménko libovolné permutace je ovšem rovno $+1$ nebo -1 a proto odtud plyne $\operatorname{sgn} \pi = \operatorname{sgn} \pi^{-1}$. □

6.4 Definice determinantu matice

Motivováni úvodní částí této kapitoly (podkapitola 6.2) a vybaveni pojmem permutace (předchozí podkapitola 6.3) nyní přichází ústřední pojem této kapitoly:

Definice 6.14. *Buď $\mathbb{A}$ čtvercová matice z $T^{n,n}$. **Determinant** matice $\mathbb{A}$ je číslo definované vztahem*

$$\det \mathbb{A} = \sum_{\pi \in S_n} \operatorname{sgn}(\pi)\, a_{1,\pi(1)} a_{2,\pi(2)} \cdots a_{n,\pi(n)}. \tag{6.8}$$

Definice determinantu si zaslouží podrobnější komentář. Rozeberme nejprve podrobně výraz v definiční rovnosti (6.8). V této sumě sčítáme *přes všechny permutace z S_n*, jinak řečeno každé permutaci z množiny S_n odpovídá jeden sčítanec této sumy. Počet sčítanců je proto roven $n!$. Sčítanci sumy jsou pak součiny znaménka dané permutace π a všech prvků matice v $k$tém řádku a $\pi(k)$tém sloupci matice $\mathbb{A}$, kde k probíhá $\hat{n}$.

Determinant matice budeme často značit i alternativním způsobem (neplést s absolutní hodnotou, ta pro matice není definována):

$$|\mathbb{A}| := \det \mathbb{A}.$$

Demonstrujme si Definici č. 6.14 explicitně na případě matic typu 2×2 a 3×3. Nemělo by nás překvapit, že dostaneme výrazy na které jsme už narazili v úvodu této kapitoly.

Determinant matice 2×2

Konkrétně uvažme matici

$$\mathbb{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{R}^{2,2}.$$

Jedná se o matici, které jsme se již věnovali v motivačním úvodu této kapitoly (tedy v podkapitole 6.2). Existují pouze dvě permutace dvouprvkové množiny $\hat{2}$, konkrétně

$$\pi_1 = (1,2) \quad \text{a} \quad \pi_2 = (2,1).$$

Proto po dosazení do (6.8) dostáváme

$$\begin{aligned} \det \mathbb{A} &= \operatorname{sgn}(\pi_1)\mathbb{A}_{1,\pi_1(1)}\mathbb{A}_{2,\pi_1 2} + \operatorname{sgn}(\pi_2)\mathbb{A}_{1,\pi_2(1)}\mathbb{A}_{2,\pi_2 2} = \\ &= 1 \cdot a \cdot d + (-1) \cdot b \cdot c = ad - bc. \end{aligned} \tag{6.9}$$

To je přesně očekávaný výsledek. Vynásobíme prvky matice $\mathbb{A}$ na diagonále a odečteme součin prvků na „antidiagonále“. Právě odvozenému vzorečku (prostě jen tupé rozepsání definice) se někdy říká „křížové pravidlo“. Důvod k tomuto označení je patrný z Obrázku č. 6.1.

Příklad 6.15. *Platí*

$$\begin{vmatrix} 2 & 3 \\ -1 & 1 \end{vmatrix} = 2 \cdot 1 - (-1) \cdot 3 = 2 + 3 = 5.$$

$$\begin{array}{ccccc} \det\begin{pmatrix}a&b\\c&d\end{pmatrix} & = & ad & - & bc \\ & & \uparrow & & \uparrow \\ & & \begin{pmatrix}\boxed{a}&b\\c&\boxed{d}\end{pmatrix} & & \begin{pmatrix}a&\boxed{b}\\\boxed{c}&d\end{pmatrix}\end{array}$$

$$\begin{array}{ccccccc} & & \begin{pmatrix}\boxed{a}&b&c\\d&\boxed{e}&f\\g&h&\boxed{j}\end{pmatrix} & & \begin{pmatrix}a&b&\boxed{c}\\\boxed{d}&e&f\\g&\boxed{h}&j\end{pmatrix} & & \begin{pmatrix}a&\boxed{b}&c\\d&e&\boxed{f}\\\boxed{g}&h&j\end{pmatrix} \\ & & \downarrow & & \downarrow & & \downarrow \\ \det\begin{pmatrix}a&b&c\\d&e&f\\g&h&j\end{pmatrix} & = & aej & + & dhc & + & gbf \\ & - & gec & - & haf & - & dbj \\ & & \uparrow & & \uparrow & & \uparrow \\ & & \begin{pmatrix}a&b&\boxed{c}\\d&\boxed{e}&f\\\boxed{g}&h&j\end{pmatrix} & & \begin{pmatrix}\boxed{a}&b&c\\d&e&\boxed{f}\\g&\boxed{h}&j\end{pmatrix} & & \begin{pmatrix}a&\boxed{b}&c\\\boxed{d}&e&f\\g&h&\boxed{j}\end{pmatrix}\end{array}$$

Obrázek 6.1: Grafické znázornění křížového a Sarrusova pravidla.

Determinant matice 3×3

Dále uvažme matici

$$\mathbb{A} = \begin{pmatrix}a&b&c\\d&e&f\\g&h&j\end{pmatrix} \in \mathbb{R}^{3,3}.$$

Nyní $n = 3$ a S_3 obsahuje $3! = 6$ permutací

$$\begin{aligned} \pi_1 &= (1,2,3), & \pi_2 &= (2,1,3), \\ \pi_3 &= (2,3,1), & \pi_4 &= (3,2,1), \\ \pi_5 &= (3,1,2), & \pi_6 &= (1,3,2). \end{aligned}$$

Permutace v levém sloupečku mají kladné znaménko a v pravém sloupečku záporné znaménko. Přímo z definice proto dostáváme

$$\det \mathbb{A} = aej + dhc + gbf - gec - haf - dbj. \tag{6.10}$$

Tento vzoreček pro výpočet determinantu matice 3×3 je známý jako „Sarrusovo pravidlo“. Jeho grafická reprezentace je uvedena na Obrázku č. 6.1. Vzorec si lze na základě této grafické ilustrace zapamatovat poměrně snadno. Členy s kladným (resp. záporným) znaménkem získáme cyklickým posunováním diagonály (resp. antidiagonály) po matici $\mathbb{A}$.

Příklad 6.16. *Platí*

$$\begin{vmatrix} 1 & 2 & 3 \\ 1 & 0 & -1 \\ 3 & 2 & 1 \end{vmatrix} = 0 + 6 - 6 - 0 - (-2) - 2 = 0.$$

Poznámka 6.17. *Hned na tomto místě zdůrazněme, že analog křížového, ani Sarrusova, pravidla neplatí pro matice větších rozměrů. Jako příklad vezměme matici*

$$\mathbb{A} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Jediná permutace $\pi \in S_4$, která nám dá nenulový sčítanec v definiční sumě (6.8) je $\pi = (2, 1, 3, 4)$. Tato permutace má znaménko rovné -1 a proto $\det \mathbb{A} = -1^4 = -1$. Kdybychom ovšem brali pouze „křížové“ součiny prvků, dostali bychom $\det \mathbb{A} = 0$. To by nemělo být překvapivé. Křížem na způsob Sarrusova pravidla vyčerpáme v tomto případě pouze $4 + 4 = 8$ permutací. Množina S_4 má ale $4! = 24$ prvků!

Poznámka 6.18. *Z výše uvedené analýzy případů matic typu 2×2 a 3×3 je jasné, že používat pouze definici determinantu na výpočet determinantů matic vyšších řádů bude nepraktické. Počet sčítanců drasticky roste s rozměrem matice (jako faktoriál!). V další části kapitoly se budeme soustředit na nalezení efektivnějšího algoritmu pro výpočet determinantu.*

Další komentáře k definici determinantu

V tento okamžik je snad milému čtenáři význam sumy v rovnici (6.8) zřejmý a je mu jasné co si pod ním má představit. Než se pustíme do studia vlastností determinantu tak je dobré uvést dvě tvrzení plynoucí takřka okamžitě z definice determinantu (Definice č. 6.14).

Tvrzení 6.19. *Mějme matici $\mathbb{A} \in T^{n,n}$.*

(i) Je-li některý ze sloupců nebo řádků matice $\mathbb{A}$ nulový, pak je determinant matice $\mathbb{A}$ roven 0.

(ii) Je-li matice $\mathbb{A}$ horní trojúhelníková[4] (tj. $\mathbb{A}_{ij} = 0$ kdykoliv $i > j$) pak

$$\det \mathbb{A} = \prod_{i=1}^{n} \mathbb{A}_{ii}.$$

Důkaz. Postupně dokážeme oba body.

(i) Za uvedeného předpokladu je v každém sčítanci v (6.8) alespoň jeden prvek, který je nulový. Suma v (6.8) je proto součtem $n!$ nul, což je nula.

[4]Například každá matice $\mathbb{A} \in T^{n,n}$ v horním stupňovitém tvaru je horní trojúhelníková.

(ii) Je jasné, že uvedený součin se v sumě (6.8) vždy vyskytuje (odpovídá identické permutaci, která je sudá). Pro každou neidentickou permutaci π ovšem existuje $k \in \hat{n}$ takové, že $k > \pi(k)$. Jinak řečeno, v každém sčítanci, který neodpovídá identické permutaci, je alespoň jeden prvek matice pod diagonálou, což je nula.

$\square$

Příklad 6.20. ***Bez jakéhokoliv počítání*** *platí*

$$\det \begin{pmatrix} 2 & 0 & 1 \\ -1 & 0 & 7 \\ 2 & 0 & 2 \end{pmatrix} = 0 \quad \textit{nebo} \quad \det \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 0 \\ 5 & 6 & 7 & 8 \\ 10 & 11 & 12 & 13 \end{pmatrix} = 0.$$

S drobným počítáním platí

$$\det \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 2 & 723 & -1 \\ 0 & 0 & 7 & 8 \\ 0 & 0 & 0 & -1 \end{pmatrix} = 1 \cdot 2 \cdot 7 \cdot (-1) = -14.$$

Determinant jednotkové matice $\mathbb{E}$ *je roven* 1,

$$\det \mathbb{E} = \det \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & & \cdots & 1 \end{pmatrix} = 1 \cdot 1 \cdots 1 = 1.$$

Z bodu (ii) předchozího tvrzení je zřejmé, že podaří-li se nám převést matici $\mathbb{A}$, jejíž determinant počítáme, do horního stupňovitého tvaru pomocí GEM a budeme-li současně vědět jak se determinant chová k úpravám GEM, tak máme vyhráno. Této výpočetní strategii se budeme věnovat v další části textu.

6.5 Vlastnosti determinantu matice

Začněme nejprve jednodušším pozorováním z něhož poté odvodíme, jak se determinant chová vůči úpravám GEM.

Věta 6.21. *Nechť* $\mathbb{A} \in T^{n,n}$.

(i) Buď $\mathbb{B}$ *matice, která vznikne z matice* $\mathbb{A}$ *prohozením itého a jtého sloupce (nebo řádku),* $i \neq j$*, potom*

$$\det \mathbb{B} = -\det \mathbb{A}.$$

(ii) Buď $\mathbb{B}$ *matice, která vznikne z matice* $\mathbb{A}$ *vynásobením itého řádku číslem* $\alpha \in T$*, potom*

$$\det \mathbb{B} = \alpha \det \mathbb{A}.$$

(iii) Buďte $\mathbb{B}$ *a* $\mathbb{D}$ *matice, které mají shodné prvky s maticí* $\mathbb{A}$ *až na itý řádek, pro který platí* $\mathbb{A}_{i:} = \mathbb{B}_{i:} + \mathbb{D}_{i:}$*, potom*

$$\det \mathbb{B} + \det \mathbb{D} = \det \mathbb{A}.$$

Ještě než se pustíme do důkazu této věty čtenáři prozradíme, že tvrzení (ii) a (iii) také platí i pro sloupce. Tento fakt okamžitě plyne z těchto bodů a z Věty č. 6.23, kterou dokážeme zanedlouho.

Důkaz. Postupně dokážeme jednotlivé body.

(i) Nechť matice $\mathbb{B} \in T^{n,n}$ vznikla z $\mathbb{A} \in T^{n,n}$ prohozením $i$tého a $j$tého sloupce a $i \neq j$. Potom pro každé $k, \ell \in \hat{n}$ platí

$$\mathbb{B}_{k\ell} = \mathbb{A}_{k,\tau_{ij}(\ell)}.$$

Zde se držíme značení zavedeného v podkapitole 6.3. Permutace τ_{ij} představuje transpozici prohazující i a j. S využitím rovnice (6.6) dostáváme

$$\begin{aligned}
\det \mathbb{B} &= \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \mathbb{B}_{1,\pi(1)} \mathbb{B}_{2,\pi(2)} \cdots \mathbb{B}_{n,\pi(n)} = \\
&= \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \mathbb{A}_{1,\tau_{ij}(\pi(1))} \mathbb{A}_{2,\tau_{ij}(\pi(2))} \cdots \mathbb{A}_{n,\tau_{ij}(\pi(n))} = \\
&= \sum_{\sigma \in S_n} \underbrace{\operatorname{sgn}(\tau_{i,j} \circ \sigma)}_{-\operatorname{sgn}(\sigma)} \mathbb{A}_{1,\sigma(1)} \mathbb{A}_{2,\sigma(2)} \cdots \mathbb{A}_{n,\sigma(n)} = -\det \mathbb{A}.
\end{aligned}$$

Zde jsme využili Tvrzení č. 6.5 a jeho důsledek pro součty přes všechny permutace. Dále jsme použili větu o chování znaménka permutace vůči skládání permutací (Věta č. 6.11). Zcela analogicky bychom ověřili tvrzení o řádcích matice $\mathbb{A}$.

(ii) Podobně jako v předchozím příkladě pro matici $\mathbb{B} \in T^{n,n}$ vzniknuvší z matice $\mathbb{A} \in T^{n,n}$ vynásobením jejího $i$tého řádku číslem α platí

$$\mathbb{B}_{k\ell} = \begin{cases} \mathbb{A}_{k\ell}, & k \neq i, \\ \alpha \mathbb{A}_{k\ell}, & k = i, \end{cases}$$

pro všechna $k, \ell \in \hat{n}$. Potom

$$\begin{aligned}
\det \mathbb{B} &= \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \mathbb{B}_{1,\pi(1)} \mathbb{B}_{2,\pi(2)} \cdots \mathbb{B}_{i,\pi(i)} \cdots \mathbb{B}_{n,\pi(n)} = \\
&= \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \mathbb{A}_{1,\pi(1)} \mathbb{A}_{2,\pi(2)} \cdots \alpha \mathbb{A}_{i,\pi(i)} \cdots \mathbb{A}_{n,\pi(n)} = \\
&= \alpha \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \mathbb{A}_{1,\pi(1)} \mathbb{A}_{2,\pi(2)} \cdots \mathbb{A}_{i,\pi(i)} \cdots \mathbb{A}_{n,\pi(n)} = \alpha \det \mathbb{A}.
\end{aligned}$$

(iii) Nechť tedy matice $\mathbb{B} \in T^{n,n}$ a matice $\mathbb{D} \in T^{n,n}$ jsou shodné až na $i$tý řádek s maticí $\mathbb{A} \in T^{n,n}$ a součet $i$tého řádku matice $\mathbb{B}$ a $i$tého řádku matice $\mathbb{D}$ je roven $i$tému řádku matice $\mathbb{A}$, $\mathbb{A}_{i:} = \mathbb{B}_{i:} + \mathbb{D}_{i:}$. Potom přímočarým výpočtem dostáváme

$$\begin{aligned}\det \mathbb{A} &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi)\mathbb{A}_{1,\pi(1)}\mathbb{A}_{2,\pi(2)}\cdots\mathbb{A}_{i,\pi(i)}\cdots\mathbb{A}_{n,\pi(n)} = \\ &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi)\mathbb{A}_{1,\pi(1)}\mathbb{A}_{2,\pi(2)}\cdots(\mathbb{B}_{i,\pi(i)}+\mathbb{D}_{i,\pi(i)})\cdots\mathbb{A}_{n,\pi(n)} = \\ &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi)\mathbb{B}_{1,\pi(1)}\mathbb{B}_{2,\pi(2)}\cdots\mathbb{B}_{i,\pi(i)}\cdots\mathbb{B}_{n,\pi(n)}+ \\ &+ \sum_{\pi\in S_n} \operatorname{sgn}(\pi)\mathbb{D}_{1,\pi(1)}\mathbb{D}_{2,\pi(2)}\cdots\mathbb{D}_{i,\pi(i)}\cdots\mathbb{D}_{n,\pi(n)} = \\ &= \det\mathbb{B}+\det\mathbb{D}.\end{aligned}$$

Věta je tím nyní dokázána. □

Poznámka 6.22. *Body (ii) a (iii) předchozí věty vlastně říkají, že je-li dáno $i \in \hat{n}$ a díváme-li se na determinant jakožto na funkci itého řádku matice, tak toto zobrazení je lineární zobrazení $T^n \to T$. Tj. jsou-li dány $i \in \hat{n}$, řádkové vektory $x_1, \cdots, x_{i-1}, x_{i+1}, x_n, x, y \in T^n$ a $\alpha \in T$ pak*

$$\det\begin{pmatrix} x_1 \\ \vdots \\ x_{i-1} \\ x+\alpha y \\ x_{i+1} \\ \vdots \\ x_n \end{pmatrix} = \det\begin{pmatrix} x_1 \\ \vdots \\ x_{i-1} \\ x \\ x_{i+1} \\ \vdots \\ x_n \end{pmatrix} + \alpha\det\begin{pmatrix} x_1 \\ \vdots \\ x_{i-1} \\ y \\ x_{i+1} \\ \vdots \\ x_n \end{pmatrix}.$$

Jakmile budeme mít dokázánu Větu č. 6.23 tak analogická poznámka platí i pro sloupce determinantu.

Následující věta, kterou jsme již v textu několikrát inzerovali, říká, že determinant matice a matice k ní transponované jsou shodné. Jak je již bylo zmíněno, tato věta nám umožňuje různá tvrzení platná pro řádky převádět na tvrzení o sloupcích determinantu a naopak.

Věta 6.23. *Pro matici $\mathbb{A} \in T^{n,n}$ platí*

$$\det\mathbb{A} = \det\mathbb{A}^T.$$

Důkaz. Pro determinant matice transponované podle definice determinantu 6.14 platí

$$\begin{aligned}\det\mathbb{A}^T &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi)\mathbb{A}^T_{1,\pi(1)}\mathbb{A}^T_{2,\pi(2)}\cdots\mathbb{A}^T_{n,\pi(n)} = \\ &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi)\mathbb{A}_{\pi(1),1}\mathbb{A}_{\pi(2),2}\cdots\mathbb{A}_{\pi(n),n} = \\ &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi)\mathbb{A}_{1,\pi^{-1}(1)}\mathbb{A}_{2,\pi^{-1}(2)}\cdots\mathbb{A}_{n,\pi^{-1}(n)} = \\ &= \sum_{\sigma\in S_n} \underbrace{\operatorname{sgn}(\sigma^{-1})}_{=\operatorname{sgn}\sigma}\mathbb{A}_{1,\sigma(1)}\mathbb{A}_{2,\sigma(2)}\cdots\mathbb{A}_{n,\sigma(n)} = \det\mathbb{A}.\end{aligned}$$

Přechod mezi druhým a třetím řádkem lze chápat takto: pro danou permutaci $\pi \in S_n$ lze členy v součinu $\mathbb{A}_{\pi(1),1} \cdots \mathbb{A}_{\pi(n),1}$ zcela jistě seřadit podle první složky ($H_\pi = \hat{n}$). Tj. pro nějaké $k \in \hat{n}$ je v tomto součinu zcela jistě člen takový, že $\pi(k) = 1$, pak ovšem pro sloupcový index tohoto členu platí $k = \pi^{-1}(1)$. Podobnou úvahou si rozmyslíme další členy v součinu (druhý až $n$tý).

Přechod mezi třetím a posledním řádkem je vlastně změna sčítacího „indexu“. Pokud $\pi = \sigma^{-1}$ a σ probíhá celou množinu S_n, pak π také proběhne celou množinu S_n, viz Tvrzení č. 6.5 a jeho důsledek. $\square$

Determinant a GEM

Z Věty č. 6.21 nyní plyne několik dalších užitečných tvrzení o vztahu determinantu a ekvivalentních úpravách GEM.

Důsledek 6.24. *Následující tvrzení jsou pravdivá.*

(i) Obsahuje-li matice dva stejné řádky, pak je její determinant nulový.

(ii) Buď $\mathbb{B}$ matice, která má všechny řádky stejné jako $\mathbb{A}$ s výjimkou $i$tého řádku, kde platí $\mathbb{B}_{i:} = \mathbb{A}_{i:} + \alpha \mathbb{A}_{j:}$ pro nějaké $\alpha \in T$, potom

$$\det \mathbb{B} = \det \mathbb{A}.$$

Speciálně[5], přičteme-li k nějakému řádku matice jiný řádek té samé matice, pak se determinant matice nezmění.

(iii) Kroky GEM mohou měnit hodnotu i znaménko determinantu, ale zachovávají nenulovost: Platí-li $\mathbb{A} \sim \mathbb{B}$, pak $\det \mathbb{A} \neq 0$, právě když $\det \mathbb{B} \neq 0$.

Důkaz. Postupně si promysleme všechna tvrzení.

(i) Nechť matice $\mathbb{A}$ má stejný $i$tý a $j$tý řádek, $i \neq j$. Prohodíme-li u takovéto matice $i$tý a $j$tý řádek, tak dostaneme stejnou matici! Podle bodu (i) Věty č. 6.21 proto platí

$$\det \mathbb{A} = -\det \mathbb{A}$$

a proto $2 \det \mathbb{A} = 0$, neboli $\det \mathbb{A} = 0$.

(ii) Nechť tedy matice $\mathbb{B}$ je totožná s maticí $\mathbb{A}$ až na $i$tý řádek matice $\mathbb{A}$, který je součtem jejího $i$tého řádku a α násobku $j$tého řádku. Potom podle bodu (iii) Věty č. 6.21 platí

$$\det \mathbb{B} = \det \mathbb{A} + \det \mathbb{A}',$$

kde $\mathbb{A}'$ je matice shodná s maticí $\mathbb{A}$ až na $i$tý řádek, který je α násobkem $j$tého řádku. Podle bodu (ii) Věty č. 6.21 pak ovšem platí

$$\det \mathbb{A}' = \alpha \det \mathbb{A}'',$$

kde matice $\mathbb{A}''$ je opět shodná s maticí $\mathbb{A}$ až na $i$tý řádek, který je roven $j$tému řádku matice $\mathbb{A}$. Podle bodu (i) Věty č. 6.21 je $\det \mathbb{A}''$ nulový jelikož má dva řádky stejné. Celkem tedy máme

$$\det \mathbb{B} = \det \mathbb{A} + \det \mathbb{A}' = \det \mathbb{A} + \alpha \det \mathbb{A}'' = \det \mathbb{A} + \alpha \cdot 0 = \det \mathbb{A}.$$

[5] Tj. pokud $\alpha = 1$

(iii) Jde o okamžitý důsledek předchozího bodu a Věty č. 6.21. □

Poznámka 6.25. *GEM lze dělat tak, že se determinant nezmění vůbec (při prohazování řádků jeden řádek vynásobit* -1 *a jinak samotné násobení řádku nenulovým číslem vůbec nepoužívat). Přičtení násobku řádku k* jinému *řádku dle předchozí věty možné je.*

Příklad 6.26. *Demonstrujme předchozí poznámku na jednoduchém příkladě matice*

$$\det \mathbb{A} = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}.$$

Nejprve pomocí definice ihned nahlédneme, že

$$\det \mathbb{A} = 4 - 3 = 1.$$

Nyní si představme, že bychom chtěli nejprve matici zjednodušit tak, aby v levém dolním políčku měla 0 *(tj. chtěli bychom ji pomocí GEM převést na horní stupňovitý tvar, to bude jedna z možných strategií výpočtu determinantu probíraná v podkapitole 6.6).*

Při převodu na horní stupňovitý tvar by bylo v pořádku k dvojnásobku druhého řádku přičíst -3 *násobek prvního řádku, tj.*

$$\mathbb{A} \sim \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} =: \mathbb{B}.$$

Pro determinanty těchto matic ovšem neplatí rovnost!

$$\det \mathbb{A} = 1 \quad a \quad \det \mathbb{B} = 2.$$

Zádrhel je v násobení řádku ke kterému pak přičítáme jiný řádek. Správně bychom museli postupovat ve dvou krocích takto:

$$\det \mathbb{A} = \frac{1}{2} \begin{vmatrix} 2 & 1 \\ 6 & 4 \end{vmatrix} = \frac{1}{2} \begin{vmatrix} 2 & 1 \\ 0 & 1 \end{vmatrix} = \frac{1}{2} \cdot 2 = 1.$$

Nejprve jsme použili bod (ii) Věty č. 6.21 na druhý řádek a poté jsme k druhému řádku přičetli -3 *násobek prvního řádku a využili bod (ii) Důsledku č. 6.24.*

Alternativně bychom se mohli násobení upravovaného řádku zcela vyhnout, přesně v duchu předchozí poznámky:

$$\det \mathbb{A} = \begin{vmatrix} 2 & 1 \\ 0 & \frac{1}{2} \end{vmatrix} = 1.$$

K druhému řádku matice $\mathbb{A}$ *jsme přičetli* $-\frac{3}{2}$ *násobek prvního řádku.*

Determinant a regularita

Nyní zformulujeme větu, kterou jsme již tušili v úvodní motivační podkapitole. Nenulovost determinantu odpovídá jednoznačné řešitelnosti soustavy $\mathbb{A}\mathbb{x} = \mathbb{b}$ s čtvercovou maticí $\mathbb{A}$ a tedy regularitě matice $\mathbb{A}$.

Věta 6.27. *Matice $\mathbb{A} \in T^{n,n}$ je regulární, právě když má nenulový determinant.*

Důkaz. Předpokládejme, že $\mathbb{A} \in T^{n,n}$ je regulární, má tedy hodnost n. Potom lze matici $\mathbb{A}$ převést pomocí ekvivalentních GEM úprav na jednotkovou matici, tj. $\mathbb{A} \sim \mathbb{E}$. Víme, že $\det \mathbb{E} = 1 \neq 0$ a proto z bodu (iii) Důsledku č. 6.24 plyne i $\det \mathbb{A} \neq 0$.

Předpokládejme naopak, že $\mathbb{A}$ není regulární a její hodnost je tedy ostře menší než n. Potom ji lze pomocí ekvivalentních úprav GEM převést na matici $\mathbb{B}$, která má poslední řádek nulový. Takováto matice $\mathbb{B}$ má dle bodu (i) Tvrzení č. 6.19 nulový determinant. Z bodu (iii) Důsledku č. 6.24 pak nutně plyne i $\det \mathbb{A} = 0$. ☐

Regulární matice mají tedy nenulový determinant. Přirozeně se nabízí otázka, jestli je nějaký vztah mezi determinantem regulární matice a matice k ní inverzní. Můžeme říci dokonce víc, determinant oplývá následující jednoduchou vlastností vůči maticovému násobení.

Věta 6.28. *Pro matice $\mathbb{A}$ a $\mathbb{B}$ z $T^{n,n}$ platí*

$$\det(\mathbb{A}\mathbb{B}) = \det \mathbb{A} \cdot \det \mathbb{B}. \tag{6.11}$$

Nejprve si dokažme jednodušší pomocné tvrzení.

Lemma 6.29. *Pro každou matici $\mathbb{D} \in T^{n,n}$ a libovolnou matici $\mathbb{P}$ reprezentující elementární krok GEM*[6] *platí*

$$\det(\mathbb{P}\mathbb{D}) = \det \mathbb{P} \cdot \det \mathbb{D}.$$

Důkaz. Stačí si uvědomit, že v předchozí podkapitole jsme toto tvrzení už prakticky odvodili. Jen si musíme rozmyslet, jak je to s determinantem matice $\mathbb{P}$. Postupně projdeme všechny tři možné případy.

- $\mathbb{P}$ představuje prohození $i$tého a $j$tého řádku, $i \neq j$. Podle bodu (i) Věty 6.21 platí $\det(\mathbb{P}\mathbb{D}) = -\det \mathbb{D}$. Matice $\mathbb{P}$ se od jednotkové matice $\mathbb{E}$ liší pouze prohozením $i$tého a $j$tého sloupce a proto v definici bude nenulový pouze člen odpovídající takovéto transpozici a tedy $\det \mathbb{P} = -1$. Dokazovaná rovnost v tomto případě platí.

- $\mathbb{P}$ představuje vynásobení $i$tého řádku nenulovým číslem α. Podle bodu (ii) Věty 6.21 platí $\det(\mathbb{P}\mathbb{D}) = \alpha \det \mathbb{D}$. Matice $\mathbb{P}$ se od jednotkové matice $\mathbb{E}$ liší pouze hodnotou $\mathbb{P}_{ii} = \alpha$ a proto $\det \mathbb{P} = \alpha$. Dokazovaná rovnost v tomto případě platí.

[6] Viz podkapitola 3.3, část Maticová interpretace GEM.

- $\mathbb{P}$ představuje přičtení α násobku $i$tého řádku k $j$tému řádku, $i \neq j$. Podle bodu (ii) Důsledku 6.24 platí $\det(\mathbb{PD}) = \det \mathbb{D}$. Matice $\mathbb{P}$ se od jednotkové matice $\mathbb{E}$ liší pouze hodnotou $\mathbb{P}_{ji} = \alpha$ a jedná se proto o matici v horním nebo dolním trojúhelníkovém tvaru pro kterou platí $\det \mathbb{P} = 1$. Dokazovaná rovnost v tomto případě platí. □

Důkaz Věty 6.28. Důkaz rozdělíme na dva případy dle regularity matice $\mathbb{A}$.

Nejprve předpokládejme, že matice $\mathbb{A}$ není regulární. Podle předchozí věty pak platí $\det \mathbb{A} = 0$. Dále z Poznámky 3.18 plyne lineární závislost souboru sloupců matice $\mathbb{A}$. Sloupce matice $\mathbb{AB}$ jsou ovšem lineární kombinace sloupců matice $\mathbb{A}$ (viz Věta č. 2.39), tj. i soubor sloupců matice $\mathbb{AB}$ je lineárně závislý a matice $\mathbb{AB}$ proto není regulární. Odtud plyne $\det(\mathbb{AB}) = 0$. Rovnost (6.11) proto v tomto případě platí ve tvaru $0 = 0$.

Nyní uvažme regulární matici $\mathbb{A}$. Z bodu (iv) Věty 3.17 víme, že $\mathbb{A} \sim \mathbb{E}$. Podle Důsledku 3.15 (a jeho důkazu) proto existuje regulární matice $\mathbb{P}$ splňující $\mathbb{A} = \mathbb{PE} = \mathbb{P}_k \cdots \mathbb{P}_1$, kde $\mathbb{P}_1, \ldots, \mathbb{P}_k$ jsou matice reprezentující elementární kroky GEM aplikované na matici $\mathbb{A}$ (viz podkapitola 3.3, část Maticová interpretace GEM).

Použijeme-li několikrát Lemma 6.29 dostáváme rovnost

$$\det(\mathbb{AB}) = \det \mathbb{P}_k \cdots \det \mathbb{P}_1 \cdot \det \mathbb{B}.$$

Uvedené Lemma nám ale také říká

$$\det \mathbb{A} = \det \mathbb{P}_k \cdots \det \mathbb{P}_1$$

a tudíž opravdu $\det(\mathbb{AB}) = \det \mathbb{A} \det \mathbb{B}$. □

Důsledek 6.30. *Pro regulární matici $\mathbb{A}$ platí $\det \mathbb{A}^{-1} = \frac{1}{\det \mathbb{A}}$.*

Důkaz. Pro regulární matici $\mathbb{A}$ platí $\mathbb{AA}^{-1} = \mathbb{E}$. Podle Věty č. 6.28 z této rovnosti plyne

$$1 = \det \mathbb{E} = \det(\mathbb{AA}^{-1}) = \det(\mathbb{A}) \cdot \det(\mathbb{A}^{-1}).$$

Proto je $\det \mathbb{A}^{-1}$ nutně nenulový a lze jím vydělit a získat dokazované tvrzení. □

6.6 Výpočet determinantu matice

Na základě vlastností determinantu vůči úpravám GEM (Důsledek 6.24) a snadnosti výpočtu determinantu matice v horním stupňovitém tvaru (bod (ii) Věty 6.21) lze nyní sestavit základní algoritmus pro výpočet determinantu.

Výpočet determinantu pomocí GEM

Algoritmus 6.31. *Matici $\mathbb{A} \in T^{n,n}$ převedeme řádkovými úpravami GEM na matici $\mathbb{B} \in T^{n,n}$ v horním trojúhelníkovém tvaru, tj. $\mathbb{B}_{ij} = 0$ pro $i > j$. Použijeme-li během eliminace 1. nebo 2. úpravu GEM, je třeba si poznamenat, jak se změnil determinant. 3. úprava GEM determinant nemění. Pro determinant matice $\mathbb{B}$ v horním trojúhelníkovém tvaru platí*

$$\det \mathbb{B} = \prod_{i=1}^{n} \mathbb{B}_{ii}.$$

Poznámka 6.32. *Výpočetní složitost tohoto algoritmu je $O(n^3)$. To je výrazná úspora oproti výpočtu determinantu z definice, kdy je složitost $O(n!)$. Např. pro $n = 50$ je to*

$$1,25 \cdot 10^5 \text{ operací} \quad \text{namísto} \quad 3,04 \cdot 10^{64} \text{ operací.}$$

Uvedený algoritmus můžeme použít i ve sloupcové variantě. Již jsme totiž dokázali Větu č. 6.23. Navíc během výpočtu můžeme sloupcové a řádkové úpravy GEM dle libosti míchat.

Příklad 6.33. *Ilustrujme výše uvedený algoritmus podrobně na následujícím příkladě.*

$$\begin{vmatrix} 2 & 7 & 1 \\ 1 & 2 & 3 \\ 3 & -2 & 5 \end{vmatrix} \overset{1.}{=} -\begin{vmatrix} 1 & 2 & 3 \\ 2 & 7 & 1 \\ 3 & -2 & 5 \end{vmatrix} \overset{2.}{=} -\begin{vmatrix} 1 & 2 & 3 \\ 0 & 3 & -5 \\ 0 & -8 & -4 \end{vmatrix}$$
$$\overset{3.}{=} -\frac{1}{3}\begin{vmatrix} 1 & 2 & 3 \\ 0 & 3 & -5 \\ 0 & -3 \cdot 8 & -3 \cdot 4 \end{vmatrix} \overset{4.}{=} -\frac{1}{3}\begin{vmatrix} 1 & 2 & 3 \\ 0 & 3 & -5 \\ 0 & 0 & -52 \end{vmatrix}$$
$$\overset{5.}{=} -\frac{1}{3} \cdot 1 \cdot 3 \cdot (-52) = 52.$$

Postupně jsme provedli následující operace:

1. *Prohození prvního a druhého řádku, změna znaménka (Věta č. 6.21 bod (i)).*
2. *K druhému řádku jsme přičetli -2 násobek prvního řádku a k třetímu řádku jsme přičetli -3 násobek prvního řádku. Tyto úpravy hodnotu determinantu nemění (Důsledek č. 6.24 bod (ii)).*
3. *Třetí řádek jsme vynásobili číslem 3 a celý determinant jsme jím pak i podělili (viz Věta č. 6.21 bod (ii)), díky tomu v našem výpočtu stále platí rovnost.*
4. *K třetímu řádku jsme přičetli 8 násobek druhého řádku (stejná úprava jako v bodě 2.).*
5. *Matice je již v horním stupňovitém tvaru a její determinant je proto součin čísel na diagonále (Tvrzení č. 6.19 bod (ii)).*

Jakmile získá čtenář trochu cviku tak samozřejmě výpočet nemusí provádět takto dopodrobna.

Tento determinant bychom mohli vypočíst i pomocí Sarrusova pravidla. Je ovšem dobré si uvědomit, že při výpočtu Sarrusovým pravidlem je potřeba provést podstatně více číselných operací a je tedy větší pravděpodobnost chyby!

Rozvoj determinantu podle řádku a sloupce

Definice 6.34. *Nechť $\mathbb{A} \in T^{n,n}$, $n \geq 2$, $\mathbb{A} = (a_{ij})$, $k, \ell \in \hat{n}$. Nechť $\mathbb{A}(k,\ell) \in T^{n-1,n-1}$ je matice, která vznikne z $\mathbb{A}$ vynecháním ktého řádku a ℓtého sloupce. Číslo*

$$(-1)^{k+\ell} \det \mathbb{A}(k,\ell)$$

*nazýváme **algebraický doplněk** prvku $a_{k\ell}$.*

K výpočtu algebraického doplňku je potřeba spočítat determinant matice s rozměrem o jedna menším než původní matice. Následující věta ukazuje, jak výpočet determinantu převést na součet násobků jistých algebraických doplňků.

Věta 6.35 (O rozvoji determinantu podle $k$tého sloupce)**.** *Nechť $\mathbb{A} \in T^{n,n}$, $n \geq 2$ a nechť $\mathbb{A} = (a_{ij})$, $k \in \hat{n}$. Potom platí:*

$$\det \mathbb{A} = \sum_{i=1}^{n} (-1)^{i+k} a_{ik} \det \mathbb{A}(i,k).$$

Důkaz. Nejprve upravme $k$tý sloupec matice $\mathbb{A}$ následovně

$$\mathbb{A}_{:k} = \sum_{i=1}^{n} a_{ik} e_i^T,$$

kde e_i je $i$tý vektor standardní báze T^n, ekvivalentně podrobněji

$$\begin{pmatrix} a_{1k} \\ a_{2k} \\ \vdots \\ a_{nk} \end{pmatrix} = a_{1k} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \cdots + a_{1n} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Použijeme-li nyní Poznámku 6.22 aplikovanou na $k$tý sloupec matice $\mathbb{A}$ dostaneme

$$\det \mathbb{A} = \sum_{i=1}^{n} a_{ik} \det \mathbb{B}[i,k],$$

kde $\mathbb{B}[i,k]$ je matice shodná s maticí $\mathbb{A}$ až na $k$tý sloupec, v němž je vektor e_i^T, tj. $\mathbb{B}[i,k] = (\mathbb{A}_{:1}, \ldots, \mathbb{A}_{:,k-1}, e_i, \mathbb{A}_{:,k+1}, \ldots, A_{:n})$. K dokončení důkazu zbývá ověřit, že

$$\det \mathbb{B}[i,k] = (-1)^{i+k} \det \mathbb{A}(i,k).$$

Pro větší názornost rozepišme matici, jejíž determinant počítáme (1 v $k$tém sloupci je v $i$tém řádku),

$$\det \mathbb{B}[i,k] = \begin{vmatrix} a_{1,1} & \cdots & a_{1,k-1} & 0 & a_{1,k+1} & \cdots & a_{1,n} \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{i,1} & \cdots & a_{i,k-1} & 1 & a_{i,k+1} & \cdots & a_{i,n} \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,k-1} & 0 & a_{n,k+1} & \cdots & a_{n,n} \end{vmatrix}.$$

Nyní použijme první bod Věty 6.21 a prohoďme řádky a sloupce tak, aby se 1 v $k$tém sloupci a $i$tém řádku dostala do levého horního rohu a *ostatní řádky a sloupce byly uspořádány jako v původní matici.* K tomu zřejmě potřebujeme $i-1$ prohození řádků a $k-1$ prohození sloupců[7], celkem se proto determinant při těchto úpravách změní

[7] Představte si, že řádek s jedničkou nejprve „probublá“ do prvního řádku a pak sloupec s jedničkou „probublá“ do prvního sloupce.

o faktor $(-1)^{i-1}(-1)^{k-1} = (-1)^{i+k}$. Platí tedy rovnost

$$\det \mathbb{B}[i,k] = (-1)^{i+k} \begin{vmatrix} 1 & a_{i,1} & \cdots & a_{i,k-1} & a_{i,k+1} & \cdots & a_{i,n} \\ 0 & a_{1,1} & \cdots & a_{1,k-1} & a_{1,k+1} & \cdots & a_{1,n} \\ & \vdots & & \vdots & \vdots & & \vdots \\ 0 & a_{i-1,1} & \cdots & a_{i-1,k-1} & a_{i-1,k+1} & \cdots & a_{i-1,n} \\ 0 & a_{i+1,1} & \cdots & a_{i+1,k-1} & a_{i+1,k+1} & \cdots & a_{i+1,n} \\ & \vdots & & \vdots & \vdots & & \vdots \\ 0 & a_{n,1} & \cdots & a_{n,k-1} & a_{n,k+1} & \cdots & a_{n,n} \end{vmatrix}.$$

Nyní si stačí uvědomit, že rozepíšeme-li determinant v předchozí rovnici pomocí definice (6.8), pak aby pro permutaci $\pi \in S_n$ byl příslušný sčítanec nenulový, musí platit $\pi(1) = 1$. Čili efektivně sčítáme přes všechny permutace $(2, 3, \ldots, n)$. Proto $\det \mathbb{B}[i,k] = (-1)^{i+k} \det \mathbb{A}(i,k)$ čímž je důkaz dokončen. $\square$

Poznámka 6.36. *Jelikož $\det \mathbb{A} = \det \mathbb{A}^T$, platí i obdobná věta o rozvoji podle kétého sloupce. Výpočet se použitím věty o rozvoji nemusí ve srovnáním s výpočtem z definice vůbec zjednodušit: složitost zůstává $O(n!)$. Věta o rozvoji výpočet zjednodušuje zejména v případech, kdy je v jednom řádku či sloupci hodně nul, případně v případech kdy lze v matici více nul snadno vytvořit pomocí úprav GEM.*

Příklad 6.37. *Vypočtěme následující determinant*

$$\begin{vmatrix} 1 & 2 & 0 & -1 \\ 0 & 3 & 2 & 2 \\ 2 & -2 & 0 & 1 \\ 3 & 1 & 0 & 3 \end{vmatrix} = 2 \cdot (-1)^{2+3} \begin{vmatrix} 1 & 2 & -1 \\ 2 & -2 & 1 \\ 3 & 1 & 3 \end{vmatrix} = -2 \begin{vmatrix} 1 & 0 & -1 \\ 2 & 0 & 1 \\ 3 & 7 & 3 \end{vmatrix} =$$

$$= -2 \cdot 7 \cdot (-1)^{3+2} \begin{vmatrix} 1 & -1 \\ 2 & 1 \end{vmatrix} = 14(1+2) = 42.$$

Nejprve jsme provedli rozvoj podle třetího sloupce (protože obsahoval největší počet nul). Poté jsme přičtením dvojnásobku třetího sloupce k druhému sloupci vytvořili dvě nuly ve druhém sloupci. Pak jsme provedli rozvoj podle druhého sloupce a nakonec jsme použili křížové pravidlo pro výpočet matice 2×2.

Nyní spočítáme determinant matice s parametrem. V následující kapitole budeme podobné výpočty potřebovat při hledání vlastních čísel matic.

Příklad 6.38. *V závislosti na parametru $\alpha \in \mathbb{R}$ určeme hodnotu následujícího determinantu*

$$\begin{vmatrix} 1 & \alpha & 2 & -1 \\ \alpha & 3 & 2 & 2 \\ 2 & -2 & 3 & 1 \\ 1 & 1 & 0 & 3 \end{vmatrix} = \begin{vmatrix} 1 & \alpha-1 & 2 & -4 \\ \alpha & 3-\alpha & 2 & 2-3\alpha \\ 2 & -4 & 3 & -5 \\ 1 & 0 & 0 & 0 \end{vmatrix} = (-1)^{4+1} \cdot 1 \cdot \begin{vmatrix} \alpha-1 & 2 & -4 \\ 3-\alpha & 2 & 2-3\alpha \\ -4 & 3 & -5 \end{vmatrix} =$$

$$= -\frac{1}{2} \begin{vmatrix} \alpha-1 & 2 & -4 \\ 4-2\alpha & 0 & 6-3\alpha \\ -5-3\alpha & 0 & 2 \end{vmatrix} = -\frac{1}{2} \cdot (-1)^{1+2} \cdot 2 \cdot \begin{vmatrix} 4-2\alpha & 6-3\alpha \\ -5-3\alpha & 2 \end{vmatrix} =$$

$$= 2(4-2\alpha) + (5+3\alpha)(6-3\alpha) = -9\alpha^2 - \alpha + 38.$$

Nejprve jsme přičtením vhodných násobků prvního sloupce k druhému a čtvrtému sloupci vytvořili v posledním řádku tři nulové prvky. Potom jsme přirozeně provedli rozvoj podle posledního řádku. Dále jsme pomocí řádkových úprav vytvořili dvě nuly v prostředním sloupci. Zde je nutné poznamenat, že k vytvoření nuly v posledním řádku jsme k dvojnásobku posledního řádku přičetli -3 násobek prvního řádku. Za to jsme museli determinant vynásobit $\frac{1}{2}$. Dále už proběhl jen rozvoj determinantu podle druhého sloupce a použití křížového pravidla na determinant matice 2×2.

6.7 Shrnutí vlastností determinantu

Pro pohodlí čtenáře ty nejdůležitější vlastnosti a metody výpočtu determinantu na tomto místě stručně shrneme.

- Determinant je definován jako součet (6.8). Rozepsáním definice pro matici 2×2 (resp. 3×3) získáváme „křížové“ (resp. Sarrusovo) pravidlo (viz (6.9), resp. (6.10)).
- Determinant změní znaménko prohodíme-li dva řádky či sloupce. Vynásobení řádku či sloupce číslem má za následek vynásobení determinantu stejným číslem. Přičtením násobku řádku (resp. sloupce) k jinému řádku (resp. sloupci) se determinant nezmění. (Věta č. 6.21)
- Determinant matice v horním stupňovitém tvaru je součin prvků na diagonále. (Tvrzení č. 6.19)
- Determinant matice $n \times n$ lze pomocí rozvoje podle řádku (či sloupce) převést na součet determinantů matic $(n-1) \times (n-1)$. (Věta č. 6.35)
- Determinanty matice a matice k ní transponované jsou stejné. (Věta č. 6.23)
- Matice je regulární, právě když její determinant je nenulový. (Věta č. 6.27)

Kapitola 7

Vlastní čísla a vlastní vektory

V této kapitole se budeme zabývat vlastními čísly a vlastními vektory lineárních operátorů a matic. Vlastní čísla a vlastní vektory nám jsou schopny říct řadu zajímavých informací o příslušných lineárních operátorech, resp. maticích, a tedy i o objektech, které popisují.

Než se pustíme do samotného výkladu, provedeme nejprve drobnou lingvistickou a historickou odbočkou. V anglické literatuře vlastní čísla najdete pod heslem *eigenvalue* a vlastní vektory pod heslem *eigenvector*. Čtenáři, který ovládá anglický jazyk, přijde předpona *eigen* jistě podezřelá, co to má znamenat? Ve skutečnosti se jedná o slovo pocházející z němčiny, kde *eigen* znamená *vlastní*[1]. Toto původně německé názvosloví se rozšířilo na začátku dvacátých let dvacátého století, kdy se zjistilo, že vlastní čísla a vlastní vektory hrají veledůležitou roli v kvantové mechanice, která se v té době rodila zejména v Německu (Einstein, Planck, Heisenberg, Schrödinger, aj.). Tento stav platí dodnes a student studující kvantové počítání a počítače se vlastním číslům a vektorům nevyhne. Vlastní čísla a vlastní vektory ovšem nacházejí uplatnění v mnoha oblastech přímo nesouvisejících s fyzikou (pro několik ukázek viz podkapitolu 7.5).

V celé této kapitole bude symbol V označovat vektorový prostor nad tělesem $\mathbb{C}$ a symbol V_n bude označovat vektorový prostor nad tělesem $\mathbb{C}$ dimenze $n \in \mathbb{N}$. V souladu s Definicí č. 1.17 chápeme vektory $x \in \mathbb{C}^n$ jako sloupcové vektory

7.1 Co si z této kapitoly odneseme

1. Pochopení pojmů vlastního čísla a vlastního vektoru operátoru a matice.
2. Základní metodu výpočtu vlastních čísel a vektorů operátorů a matice.
3. Význam problému diagonalizace operátoru a matice a metody jeho řešení.
4. Příklady využití vlastních čísel a vektorů operátorů a matic.

[1] Ale také *podivný* a *svérázný*. Z pohledu mnoha studentů jde tedy o výstižné označení.

7.2 Motivace

Způsobů jak motivovat zavedení vlastních čísel a vektorů lineárního operátoru (či matice) je celá řada. Většinou ovšem ze strany studentů a studentek vyžadují porozumění problému z jiné domény (fyzika, statistika,...), kde se využívají. V prvním ročníku vysokoškolského studia na informaticky zaměřené fakultě nelze mezi studenty příliš očekávat povědomí o těchto oblastech. V tomto textu proto zvolíme trochu jiný přístup k motivaci těchto dvou souvisejících pojmů. Vyjdeme z toho, co už je čtenáři známo z předcházející kapitoly o lineárních zobrazeních (Kapitola 5).

Další aplikace vlastních čísel a vlastních vektorů alespoň stručně zmíníme na závěr této kapitoly v podkapitole 7.5.

Jak analyzovat lineární operátory?

Představme si pro jednoduchost následující situaci. Máme lineární operátor A působící na prostoru $\mathbb{R}^2$. V podkapitole 5.5 jsme si ukázali, jak ke zvolené bázi $\mathcal{X}$ zkonstruovat matici operátoru A, tedy v tomto případě ${}^{\mathcal{X}}\!A = {}^{\mathcal{X}}\!A^{\mathcal{X}} \in \mathbb{R}^{2,2}$.

Matice ${}^{\mathcal{X}}\!A$ obecně závisí na volbě báze $\mathcal{X}$. Změníme-li bázi $\mathcal{X}$, tak se změní[2] i matice ${}^{\mathcal{X}}\!A$. Nemohli bychom se pokusit nalézt bázi $\mathcal{X}$ tak, aby se z příslušné matice ${}^{\mathcal{X}}\!A$ dalo vyčíst „co vlastně operátor A na prostoru $\mathbb{R}^2$ dělá“? Dále je jasné, že čím jednodušší matice ${}^{\mathcal{X}}\!A$ bude, tím snadněji se s ní pravděpodobně bude počítat. Ideální by bylo, kdyby se nám podařilo[3] nalézt bázi $\mathcal{X} = (x_1, x_2)$ prostoru $\mathbb{R}^2$ tak, aby matice zobrazení A v této bázi byla diagonální[4], tedy

$$
{}^{\mathcal{X}}\!A = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}.
$$

Pojďme si rozmyslet, co všechno můžeme v takovémto případě o operátoru A říci. Jaké důsledky z existence takovéto báze plynou? Vzpomeňme si, že $(x_1)_{\mathcal{X}} = (1, 0)$ a proto

$$
\lceil Ax_1 \rceil_{\mathcal{X}} = {}^{\mathcal{X}}\!A \cdot \lceil x_1 \rceil_{\mathcal{X}} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha \\ 0 \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \alpha \lceil x_1 \rceil_{\mathcal{X}} = \lceil \alpha x_1 \rceil_{\mathcal{X}}.
$$

Pro první bazický vektor x_1 tedy platí

$$
Ax_1 = \alpha x_1. \tag{7.1}
$$

Formální definici vlastního čísla a vektoru jsme ještě neprovedli (Definice č. 7.1), můžeme ale čtenáři prozradit, že přesně v tomto případě (myšleno (7.1)) budeme o α mluvit jako o vlastním čísle operátoru A a o x_1 jako o k němu příslušejícímu vlastnímu vektoru. Zcela analogicky bychom odvodili rovnost $Ax_2 = \beta x_2$. Tedy i β je vlastním číslem operátoru A a x_2 je příslušný vlastní vektor.

Co nám tyto dvě rovnosti říkají? Operátor A při působení na vektor x_1 tento vektor pouze vynásobí číselným faktorem α. Podobně, je-li na vstupu operátoru A vektor x_2, pak na jeho výstupu bude jeho β-násobek. Jinak řečeno, operátor ve směru vektoru x_1 (resp. x_2) provádí pouze škálování příslušnými číselnými faktory[5].

[2] S výjimkou identity a nulového zobrazení.

[3] Na konci této kapitoly uvidíme, že ne vždy takováto báze existuje.

[4] Tomuto problému se budeme podrobně věnovat na konci této kapitoly v podkapitole 7.4.

[5] Vzpomeňte na Příklad č. 5.42

Z toho dále plyne, že je-li $x = c_1x_1 + c_2x_2$ libovolný vektor z $\mathbb{R}^2$, pak

$$Ax = c_1Ax_1 + c_2Ax_2 = c_1\alpha x_1 + c_2\beta x_2.$$

Geometricky je nyní snadné si představit jak působení operátoru A probíhá, ať už byl zadán jakýmkoliv způsobem.

„Diagonálnost“ matice zobrazení ${}^{\mathcal{X}}A$ má výhody i z čistě výpočetního hlediska. Představme si, že bychom chtěli počítat mocniny operátoru A. Pracujeme-li v bázi $\mathcal{X}$ jako výše, pak je potřeba umocňovat matici ${}^{\mathcal{X}}A$. Umocňovat diagonální matici je ale extrémně jednoduché! Skutečně,

$$\left({}^{\mathcal{X}}A\right)^k = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}^k = \begin{pmatrix} \alpha^k & 0 \\ 0 & \beta^k \end{pmatrix}.$$

K docenění tohoto vzorce je nutné si představit, jak komplikované by bylo sestavit obecný předpis pro $n$tou mocninu jiné „plné“ matice (viz Příklad č. 7.5).

K výpočtu $k$té mocniny takovéto diagonální matice je tak potřeba pouze $2(k-1)$ násobení a žádné sčítání. Při výpočtu součinu dvou matic 2×2 je jinak potřeba obecně provést 8 součinů a 4 součty. Proto k výpočtu $k$té mocniny „plné“ matice je potřeba vykonat $12(k-1)$ aritmetických operací. To je šestkrát více, než v případě diagonální matice[6]!

7.3 Vlastní čísla a vlastní vektory lineárního operátoru

Základní definice a vlastnosti

Nyní formálně zavedeme pojem vlastního čísla a vlastního vektoru lineárního operátoru. Následující definice by neměla být po úvodní motivační části této kapitoly nijak překvapivá.

Definice 7.1. *Řekneme, že*[7] $\lambda \in \mathbb{C}$ *je* ***vlastní číslo operátoru*** $A \in \mathcal{L}(V)$*, právě když existuje* $x \in V$*,* $x \neq \theta$*, takový, že* $Ax = \lambda x$*. Vektor* x *pak nazýváme* ***vlastním vektorem operátoru*** A ***příslušejícím vlastnímu číslu*** λ*. Množinu všech vlastních čísel* A *nazýváme* ***spektrem operátoru*** A *a značíme symbolem*[8] $\sigma(A)$*.*

Na tomto místě ihned zmiňme častou studentskou chybku. V definici se požaduje *nenulovost* vlastního vektoru x. Pokud na nenulovost zapomenete, tak se to může zdát jako malé opomenutí a v písemce pak nula bodů zamrzí. Opak je ovšem pravdou. Kdyby v definici požadavek $x \neq \theta$ nebyl, tak se celý pojem vlastního čísla stává triviálním a bude zhola k ničemu. Proč? Protože pro *libovolné* komplexní číslo λ a libovolný lineární operátor A platí $A\theta = \lambda\theta$. Tj. spektrum libovolného operátoru by byla celá komplexní rovina. Jinak řečeno, libovolné komplexní číslo by bylo vlastním číslem libovolného lineárního operátoru, vždy by platilo $\sigma(A) = \mathbb{C}$. To by byl jistě zcela neužitečný pojem. Proto nula bodů.

[6] Laskavý čtenář si jistě sám rozmyslí, jak by tato výpočetní porovnání dopadlo v případě $n \times n$ matice.

[7] Řecké písmenko λ, *lambda*.

[8] Řecké písmenko σ, *sigma*.

Poznámka 7.2. *Dále učiňme ještě jednu terminologickou poznámku. Proč se množině vlastních čísel říká* spektrum*? Toto názvosloví opět pochází z kvantové fyziky: atomu libovolného prvku z periodické tabulky lze přiřadit jistý lineární operátor*[9]*, jehož vlastní čísla udávají energetické hladiny, na kterých se mohou pohybovat elektrony v jeho elektronovém obalu. Jinak řečeno, vlastní čísla můžeme fyzicky pozorovat ve spektrometru. Proto spektrum.*

Vzpomeňte si dále na elektronové orbitaly, o kterých se učí už ve středoškolské chemii. Tyto orbitaly lze hledat právě jako vlastní vektory jistého lineárního operátoru. Vlastní čísla a vlastní vektory máme proto doslova na dotek každým okamžikem svého života.

Nyní se pojďme zamyslet jak hledat vlastní čísla a vlastní vektory lineárního operátoru $A \in \mathcal{L}(V_n)$. Hledáme komplexní čísla $\lambda \in \mathbb{C}$, pro která existuje nenulový vektor $x \in V_n$ splňující

$$Ax = \lambda x.$$

Tuto rovnost můžeme ekvivalentně vyjádřit v následujícím tvaru[10]

$$(A - \lambda E)x = \theta.$$

Vzhledem k požadavku nenulovosti vektoru x to znamená, že operátor $A - \lambda E$ není injektivní (vzpomeňte na Pozorování č. 5.16; navíc dle Důsledku č. 5.17 není ani surjektivní). Vlastní čísla λ operátoru A jsou proto všechna komplexní čísla pro která operátor $A - \lambda E$ *není* izomorfismem V_n. Vlastní vektor příslušející takovémuto vlastnímu číslu λ je potom libovolný nenulový vektor z jádra operátoru $A - \lambda E$, tj. vektor $x \neq \theta$ splňující $(A - \lambda E)x = \theta$. Shrňme si výsledek úvahy tohoto odstavce do následující definice a tvrzení.

Definice 7.3. *Je-li $\lambda \in \mathbb{C}$ vlastní číslo operátoru $A \in \mathcal{L}(V_n)$, pak podprostor* $\ker(A - \lambda E)$ *nazýváme* ***vlastním podprostorem operátoru*** *A* ***příslušejícím vlastnímu číslu*** *λ.*

Tvrzení 7.4. *Číslo $\lambda \in \mathbb{C}$ je vlastní číslo operátoru $A \in \mathcal{L}(V_n)$, právě když operátor $A - \lambda E$ není izomorfismem. Libovolný nenulový vektor z vlastního podprostoru* $\ker(A - \lambda E)$ *je pak vlastním vektorem operátoru A příslušejícím vlastnímu číslu λ.*

Důkaz. Byl již proveden v předcházejícím odstavci. □

Zdůrazněme samostatně důležitou informaci obsaženou v předchozím tvrzení. Je-li λ vlastní číslo $A \in \mathcal{L}(V_n)$ a $x, y \in \ker(A - \lambda E)$ vlastní vektory operátoru A příslušející vlastnímu číslu λ, pak i αx je vlastní vektor pro libovolné nenulové $\alpha \in \mathbb{C}$ a součet $x + y$, je-li nenulový, je také vlastní vektor operátoru A s vlastním číslem λ. Jádro libovolného operátoru je totiž, jak už víme, podprostor.

Vlastních vektorů k vlastnímu číslu je tedy vždy nekonečně mnoho[11]. Protože ale všechny vlastní vektory (spolu s nulovým vektorem) tvoří podprostor, má smysl „množství" vlastních vektorů vyjádřit pomocí dimenze vlastního podprostoru, resp. pomocí následujícího pojmu.

[9] Definovaný ovšem na prostoru nekonečné dimenze.

[10] Operátor E označuje identitu na V_n, pro všechna $v \in V_n$ platí $Ev = v$.

[11] Nezapomínejte, že v této kapitole pracujeme nad tělesem $\mathbb{C}$!

Definice 7.5. *Nechť $\lambda \in \mathbb{C}$ je vlastní číslo operátoru $A \in \mathcal{L}(V_n)$. Číslo $d(A - \lambda E) = \dim\ker(A - \lambda E)$ nazýváme* ***geometrickou násobností vlastního čísla*** *λ a značíme*[12] *ji*[13] *$\nu_g(\lambda)$.*

Geometrická násobnost vlastního čísla bude hrát důležitou roli dále v kapitole o diagonalizaci lineárních operátorů. V tento okamžik pouze poznamenejme, že geometrická násobnost libovolného vlastního čísla λ lineárního operátoru $A \in \mathcal{L}(V_n)$ zřejmě[14] splňuje

$$1 \leq \nu_g(\lambda) \leq n.$$

Výpočet vlastních čísel a vlastních vektorů operátorů

Nyní se pojďme podrobněji zamyslet jak vlastní čísla a vlastní vektory hledat. Výchozím bodem pro nás bude Tvrzení č. 7.4. Nejprve dokažme následující pomocné tvrzení.

Lemma 7.6. *Nechť $A \in \mathcal{L}(V_n)$ a $\mathcal{X}$ je báze prostoru V_n. Označme*

$$p_A(\lambda) := \det {}^{\mathcal{X}}\!(A - \lambda E), \quad \lambda \in \mathbb{C}. \tag{7.2}$$

Potom p_A je polynom stupně n a nezávisí na volbě báze $\mathcal{X}$.

Důkaz. Nejprve si rozmysleme, že takto zadefinovaná funkce p_A je skutečně polynomem. Je-li ${}^{\mathcal{X}}\!A = (a_{i,j})_{i,j=1}^{n} \in \mathbb{C}^{n,n}$, pak podle Věty č. 5.27 je ${}^{\mathcal{X}}\!(A - \lambda E) = {}^{\mathcal{X}}\!A - \lambda\mathbb{E}$ a proto

$$p_A(\lambda) = \begin{vmatrix} a_{1,1}-\lambda & a_{1,2} & a_{1,3} & \cdots & a_{1,n-1} & a_{1,n} \\ a_{2,1} & a_{2,2}-\lambda & a_{2,3} & \cdots & a_{2,n-1} & a_{2,n} \\ a_{3,1} & a_{3,2} & a_{3,3}-\lambda & & a_{3,n-1} & a_{3,n} \\ \vdots & \vdots & & \ddots & \vdots & \vdots \\ a_{n-1,1} & a_{n-1,2} & a_{n-1,3} & \cdots & a_{n-1,n-1}-\lambda & a_{n-1,n} \\ a_{n,1} & a_{n,2} & a_{n,3} & \cdots & a_{n,n-1} & a_{n,n}-\lambda \end{vmatrix}. \tag{7.3}$$

Nyní si stačí vybavit definici determinantu (Definice č. 6.14). Podle ní je determinant na pravé straně rovnice (7.3) skutečně polynomem v proměnné λ (ano, jde o jistý součet číselných násobků součinů prvků výše uvedené matice). Zároveň z ní plyne, že člen obsahující největší mocninu λ je ten odpovídající identické permutaci a je roven

$$\prod_{j=1}^{n} (a_{j,j} - \lambda).$$

Proto je člen p_A s největší mocninou roven $(-1)^n \lambda^n$ a p_A je tedy polynomem stupně n.

Mějme nyní navíc bázi $\mathcal{Y}$ prostoru V_n. Potom podle Věty č. 5.39 platí

$${}^{\mathcal{X}}\!(A - \lambda E) = {}^{\mathcal{Y}}\!E^{\mathcal{X}} \cdot {}^{\mathcal{Y}}\!(A - \lambda E) \cdot {}^{\mathcal{X}}\!E^{\mathcal{Y}}$$

[12]Pozor, v tomto standardním značení je potlačena závislost na A. Při používání tohoto symbolu musí být vždy jasné, o jakém operátoru mluvíme.

[13]Řecké písmenko ν, *ný*.

[14]Vlastní podprostor má dimenzi nejméně 1 a nejvýše n, což je dimenze V_n.

Dále si připomeňme Větu č. 5.35 zajišťující rovnost ${}^{\mathcal{Y}}E^{\mathcal{X}} = \left({}^{\mathcal{X}}E^{\mathcal{Y}}\right)^{-1}$. Konečně pak podle Věty č. 6.28 o vztahu determinantu a maticového násobení platí

$$\begin{aligned} p_A(\lambda) &= \det {}^{\mathcal{X}}(A-\lambda E) = \det\left({}^{\mathcal{Y}}E^{\mathcal{X}} \cdot {}^{\mathcal{Y}}(A-\lambda E) \cdot {}^{\mathcal{X}}E^{\mathcal{Y}}\right) = \\ &= \det\left({}^{\mathcal{Y}}E^{\mathcal{X}}\right) \cdot \det\left({}^{\mathcal{Y}}(A-\lambda E)\right) \cdot \det\left({}^{\mathcal{X}}E^{\mathcal{Y}}\right) = \\ &= \frac{1}{\det\left({}^{\mathcal{X}}E^{\mathcal{Y}}\right)} \cdot \det\left({}^{\mathcal{Y}}(A-\lambda E)\right) \cdot \det\left({}^{\mathcal{X}}E^{\mathcal{Y}}\right) = \det\left({}^{\mathcal{Y}}(A-\lambda E)\right). \end{aligned}$$

Ve výpočtu jsme ještě použili Větu č. 6.30 o determinantu inverzní matice. □

Nyní má smysl zadefinovat následující pojem bez reference na bázi prostoru V_n.

Definice 7.7. *Polynom p_A z předchozího tvrzení (konkrétně rovnice (7.2)) nazýváme* ***charakteristickým polynomem operátoru*** *A.*

Zdůrazněme, že podle Lemmatu č. 7.6 je jedno pomocí jaké báze charakteristický polynom počítáme. Charakteristický polynom p_A operátoru $A \in \mathcal{L}(V_n)$ je polynom stupně n. Než se pustíme do dalšího výkladu, je vhodné připomenout si několik faktů o komplexních polynomech a jejich kořenech. Tato poznámka je proto také důvodem proč v této kapitole uvažujeme operátory na prostorech nad komplexními čísly. I když matice operátoru v jisté bázi má pouze reálné složky, může se snadno stát, že příslušný charakteristický polynom má komplexní kořeny.

Poznámka 7.8 (Komplexní polynomy)**.** *Dle tzv. Základní věty algebry pro každý komplexní polynom $p : \mathbb{C} \to \mathbb{C}$ stupně $n \in \mathbb{N}$ existují $k \in \hat{n}$, vzájemně různá komplexní čísla $\lambda_1, \ldots, \lambda_k \in \mathbb{C}$ a přirozená čísla $\ell_1, \ldots, \ell_k \in \mathbb{N}$ splňující*

$$p(z) = \alpha_n \prod_{j=1}^{k} (z-\lambda_j)^{\ell_j},$$

kde α_n je koeficient u mocniny λ^n v polynomu p a $\ell_1 + \ell_2 + \cdots + \ell_k = n$.

Čísla $\lambda_1, \ldots, \lambda_k$ jsou právě všechny ***kořeny polynomu*** *p. Z uvedené věty plyne, že komplexní polynom má alespoň jeden kořen a nejvýše jich je n. Číslo ℓ_j, $j \in \hat{k}$, nazýváme* ***násobností kořenu*** *λ_j polynomu p. Pokud bychom kořeny počítali včetně jejich násobnosti (ne jen vzájemně různé), tak bychom předchozí tvrzení mohli formulovat také tak, že každý komplexní polynom stupně $n \in \mathbb{N}$ má právě n komplexních kořenů (připouští se rovnost u vícenásobných).*

Například pro polynom

$$p(z) = 2\,z^8 + 12\,z^7 - 104\,z^6 + 368\,z^5 - 1120\,z^4 + 2368\,z^3 - 3456\,z^2 + 4352\,z - 3072$$

platí[15]

$$p(z) = 2\,(z+12)(z+2i)^2(z-2i)^2(z-2)^3.$$

Tento polynom má tedy čtyři vzájemně různé kořeny -12, $2i$, $-2i$ a 2. Kořen -12 má násobnost 1, Kořeny $2i$ a $-2i$ mají násobnost 2 a konečně kořen 2 má násobnost 3. Pokud bychom počítali kořeny včetně násobností, pak jich tento polynom má $1 + 2 + 2 + 3 = 8$, což je přesně rovno stupni polynomu p.

[15] Snadno ověříte roznásobením.

Příklad 7.9. *Uvažme operátor A mající v bázi $\mathcal{X}$ prostoru $\mathbb{C}^3$ matici*

$$^{\mathcal{X}}A = \begin{pmatrix} 1 & -1 & 1 \\ 2 & 0 & -2 \\ 3 & -1 & -1 \end{pmatrix}$$

a nalezněme jeho charakteristický polynom. V závislosti na $\lambda \in \mathbb{C}$ musíme vypočítat následující determinant

$$\begin{aligned} p_A(\lambda) &= \begin{vmatrix} 1-\lambda & -1 & 1 \\ 2 & -\lambda & -2 \\ 3 & -1 & -1-\lambda \end{vmatrix} \overset{1.}{=} \begin{vmatrix} 1-\lambda & -1 & 1 \\ 2-\lambda+\lambda^2 & 0 & -2-\lambda \\ 2+\lambda & 0 & -2-\lambda \end{vmatrix} \\ &\overset{2.}{=} (-1)^{1+2} \cdot (-1) \cdot \begin{vmatrix} 2-\lambda+\lambda^2 & -2-\lambda \\ 2+\lambda & -2-\lambda \end{vmatrix} \overset{3.}{=} (2+\lambda) \begin{vmatrix} 2-\lambda+\lambda^2 & -2-\lambda \\ 1 & -1 \end{vmatrix} \\ &\overset{4.}{=} (2+\lambda)(-2+\lambda-\lambda^2+2+\lambda) = \lambda(2+\lambda)(2-\lambda). \end{aligned}$$

Postupně jsme provedli tyto kroky:

1. *Řádkovými úpravami GEM neměnícími determinant jsme v druhém sloupci vytvořili dvě nuly.*
2. *Provedli jsme rozvoj determinantu podle druhého sloupce.*
3. *Vytkli jsme společný multiplikativní faktor z druhého řádku matice.*
4. *Použili jsme křížové pravidlo na výpočet determinantu 2×2 a výsledný polynom jsme dále faktorizovali.*

Pomocí charakteristického polynomu operátoru nyní můžeme hledat vlastní čísla operátoru! Konkrétně platí následující věta.

Věta 7.10. *Nechť $A \in \mathcal{L}(V_n)$. Potom $\sigma(A) \neq \emptyset$ a spektrum operátoru A je tvořeno všemi komplexními kořeny charakteristického polynomu p_A, tj.*

$$\sigma(A) = p_A^{-1}(\{0\}) = \{\lambda \in \mathbb{C} \mid p_A(\lambda) = 0\}.$$

Důkaz. Z Tvrzení č. 7.4 víme, že λ je vlastním číslem operátoru $A \in \mathcal{L}(V_n)$, právě když operátor $A - \lambda E$ není izomorfismem. Dle Důsledku č. 5.33 je toto ekvivalentní singularitě matice $^{\mathcal{X}}(A - \lambda E)$ v libovolné bázi $\mathcal{X}$ prostoru $\mathcal{L}(V_n)$ a tedy nulovosti jejího determinantu (Věta č. 6.27), čili rovnosti $p_A(\lambda) = 0$. Poznámka č. 7.8 zaručuje existenci alespoň jednoho kořenu polynomu p_A a tedy i neprázdnost množiny $\sigma(A)$. $\square$

Vedle geometrické násobnosti vlastního čísla dále definujeme jeho algebraickou násobnost.

Definice 7.11. *Nechť $A \in \mathcal{L}(V_n)$ a $\lambda \in \sigma(A)$. Násobnost čísla λ jako kořene charakteristického polynomu p_A operátoru A nazýváme **algebraickou násobností vlastního čísla** λ a značíme ji $\nu_a(\lambda)$.*

Pro algebraickou násobnost vlastního čísla λ operátoru A zřejmě platí $1 \leq \nu_a(\lambda) \leq n$. Následující věta ukazuje jednoduchý vztah mezi algebraickou a geometrickou násobností.

Věta 7.12. *Nechť $A \in \mathcal{L}(V_n)$, $\lambda \in \sigma(A)$. Potom $1 \leq \nu_g(\lambda) \leq \nu_a(\lambda)$.*

Důkaz. Nechť geometrická násobnost vlastního čísla[16] η operátoru $A \in \mathcal{L}(V_n)$ je rovna $k \in \hat{n}$. Lze k němu tedy nalézt k lineárně nezávislých vlastních vektorů $v_1, \dots, v_k$ operátoru A, $Av_j = \eta v_j$ pro každé $j \in \hat{k}$. Doplňme tyto vektory na bázi prostoru V_n,

$$\mathcal{X} = (v_1, \dots, v_k, v_{k+1}, \dots v_n).$$

Matice operátoru A vzhledem k této bázi pak má blokový tvar

$$^{\mathcal{X}}A = \begin{pmatrix} \eta\mathbb{E}_k & \mathbb{B}_1 \\ \Theta_k & \mathbb{B}_2 \end{pmatrix} \in \mathbb{C}^{n,n},$$

kde $\mathbb{E}_k \in \mathbb{C}^{k,k}$ je jednotková matice, $\Theta_k \in \mathbb{C}^{n-k,k}$ je nulová matice a $\mathbb{B}_1 \in \mathbb{C}^{k,n-k}$, $\mathbb{B}_2 \in \mathbb{C}^{n-k,n-k}$ jsou jisté komplexní matice. Skutečně, pro každé $j \in \hat{\{k\}}$ platí $\lceil Av_j \rceil_{\mathcal{X}} = \lceil \eta v_j \rceil_{\mathcal{X}} = (0, \dots, \eta, \dots, 0)^T$, kde η je v $j$té složce. Protože podle Lemmatu č. 7.6 charakteristický polynom operátoru A nezávisí na volbě báze, obdržíme rovnost

$$p_A(\lambda) = \det {}^{\mathcal{X}}(A - \lambda E) = \det \left({}^{\mathcal{X}}A - \lambda\mathbb{E} \right).$$

Použijeme-li při výpočtu příslušného determinantu $k$krát rozvoj (viz Větu č. 6.35) podle prvního sloupce, dostaneme

$$p_A(\lambda) = (\eta - \lambda)^k \det(\mathbb{B}_2 - \lambda\mathbb{E}).$$

Čili η je *alespoň* $k$násobným kořenem polynomu p_A, tj. $\nu_g(\lambda) = k \leq \nu_a(\lambda)$. □

Příklad 7.13. *V předchozím příkladě (Příklad č. 7.9) jsme se zabývali operátorem $A \in \mathcal{L}(V_n)$, který v bázi $\mathcal{X}$ měl matici*

$$^{\mathcal{X}}A = \begin{pmatrix} 1 & -1 & 1 \\ 2 & 0 & -2 \\ 3 & -1 & -1 \end{pmatrix}.$$

Spočetli jsme jeho charakteristický polynom,

$$p_A(\lambda) = \lambda(2 + \lambda)(2 - \lambda).$$

Podle Věty č. 7.10 pak kořeny tohoto polynomu

$$\lambda_1 = 0, \quad \lambda_2 = -2, \quad \lambda_3 = 2$$

jsou vlastní čísla operátoru A. Protože každé z těchto tří čísel je kořenem násobnosti 1 polynomu p_A, má každé z nich algebraickou násobnost 1, tj.

$$\nu_a(0) = \nu_a(-2) = \nu_a(2) = 1.$$

Díky předchozí větě (Věta č. 7.12) i bez počítání vlastních podprostorů ihned víme, že i pro geometrické násobnosti platí

$$\nu_g(0) = \nu_g(-2) = \nu_g(2) = 1.$$

[16] Řecké písmenko η, *éta*.

Příklad 7.14. *Skeptický čtenář by stále mohl mít pochyby o nutnosti pracovat s komplexními čísly. Nejsou příklady operátory s nereálnými vlastními čísly pouze exotické či okrajové? Nejsou.*

Jako příklad uvažme operátor $R \in \mathcal{L}(\mathbb{R}^2)$ představující rotaci vektorů z $\mathbb{R}^2$ vůči počátku (tj. θ) o $90°$ proti směru hodinových ručiček[17]*. K zavedení takovéhoto operátoru jistě komplexní čísla nepotřebujeme.*

Uvažme standardní bázi $\mathcal{E} = (e_1, e_2)$ prostoru $\mathbb{R}^2$. Vzhledem k definici operátoru R zřejmě platí $Re_1 = e_2$ a $Re_2 = -e_1$. Proto pro jeho matici ve standardní bázi platí

$$^{\mathcal{E}}R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Jeho charakteristickým tedy je

$$p_R(\lambda) = \begin{vmatrix} -\lambda & -1 \\ 1 & -\lambda \end{vmatrix} = \lambda^2 + 1.$$

Jeho kořeny jsou $\lambda_1 = i$ a $\lambda_2 = -i$. O rotaci určitě nelze říct, že by se jednalo o okrajový nezajímavý případ.

Příklad 7.15. *Mějme bázi $\mathcal{X} = (x_1, x_2)$ prostoru V_2 a operátor $A \in \mathcal{L}(V_n)$ jehož matice v bázi $\mathcal{X}$ je*[18]

$$^{\mathcal{X}}A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Jeho charakteristický polynom je roven

$$p_A(\lambda) = \begin{vmatrix} 1-\lambda & 1 \\ 0 & 1-\lambda \end{vmatrix} = (1-\lambda)^2.$$

Jediným vlastním číslem operátoru A je proto $\lambda_1 = 1$. Jeho algebraická násobnost je $\nu_a(1) = 2$.

Hledejme příslušný vlastní podprostor, pro matici příslušné soustavy platí

$$^{\mathcal{X}}(A - \lambda_1 E) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Pro všechna řešení soustavy $^{\mathcal{X}}(A - \lambda_1 E) \cdot \lceil x \rceil_{\mathcal{X}} = \theta$ proto platí $(x)_{\mathcal{X}} \in \langle (1,0) \rangle$, a proto $\ker(A - \lambda_1 E) = \langle x_1 \rangle$. Jinak řečeno, vlastním vektorem k vlastnímu číslu $\lambda_1 = 1$ je libovolný nenulový násobek vektoru x_1. Geometrická násobnost vlastního čísla $\lambda_1 = 1$ je pouze 1. V tomto případě mezi násobnostmi platí ostrá nerovnost $\nu_g(1) = 1 < 2 = \nu_a(1)$.

Zakončeme tuto část textu shrnutím algoritmů pro výpočet vlastních čísel a vlastních vektorů lineárního operátoru.

Algoritmus 7.16 (Výpočet vlastních čísel operátoru A a jejich algebraických násobností)**.** *Mějme lineární operátor A na prostoru V_n.*

[17] O tomto operátoru jsme se již zmiňovali v úvodu podkapitoly 5.5.

[18] Jedná se o operátor zkosení, kterým jsme se zabývali již dříve v Příkladu č. 5.43.

1. *Zvolme bázi $\mathcal{X}$ prostoru V_n.*

2. *Spočtěme charakteristický polynom operátoru A, $p_A(\lambda) = \det{}^{\mathcal{X}}(A - \lambda E)$, pomocí známých metod pro výpočet determinantu (Kapitola č. 6).*

3. *Nalezněme[19] všechny kořeny polynomu p_A. Tyto kořeny jsou vlastní čísla operátoru A.*

4. *Algebraická násobnost vlastního čísla λ, tj. $\nu_a(\lambda)$, je násobnost λ jako kořene charakteristického polynomu p_A.*

Algoritmus 7.17 (Výpočet vlastních vektorů operátoru A a geometrických násobností)**.** *Mějme lineární operátor A na prostoru V_n a jeho vlastní číslo $\lambda \in \mathbb{C}$.*

1. *Vlastní vektory příslušné vlastnímu číslu λ jsou všechna nenulová řešení rovnice $(A - \lambda E)x = \theta$.*

2. *Geometrická násobnost vlastního čísla λ, tj. $\nu_g(\lambda)$, je dimenze vlastního podprostoru* $\ker(A - \lambda E)$.

Vlastní čísla a vlastní vektory matice

Často se vyskytne situace, kdy máme operátor $A \in \mathcal{L}(\mathbb{C}^n)$ přímo zadaný pomocí matice $\mathbb{A} \in \mathbb{C}^{n,n}$ předpisem $Ax := \mathbb{A} \cdot x$ pro každé $x \in \mathbb{C}^n$, případně máme matici bez jakéhokoliv vztahu k nějakému operátoru. Potom se vyplatí zavést následující pojmy.

Definice 7.18. *Komplexní číslo λ nazýváme* ***vlastním číslem matice*** $\mathbb{A} \in \mathbb{C}^{n,n}$, *právě když existuje nenulový vektor $x \in \mathbb{C}^n$ splňující*

$$\mathbb{A} \cdot x = \lambda x.$$

Takovýto vektor x pak nazýváme ***vlastním vektorem matice*** $\mathbb{A}$ ***příslušejícím vlastnímu číslu*** λ. ***Spektrem matice*** $\mathbb{A}$ *(ozn. $\sigma(\mathbb{A})$) je množina všech vlastních čísel matice $\mathbb{A}$.* ***Charakteristický polynom matice*** $\mathbb{A}$ *(ozn. $p_{\mathbb{A}}$) definujeme předpisem*

$$p_{\mathbb{A}}(\lambda) := \det(\mathbb{A} - \lambda \mathbb{E}).$$

Takováto definice může být potenciálně matoucí. Výše uvedené pojmy máme definované pro operátory i pro matice. Nehrozí proto zmatení? Nehrozí! Pojďme si vztah těchto pojmů rozmyslet.

Mějme operátor $A \in \mathcal{L}(V_n)$ a bázi $\mathcal{X}$ prostoru V_n. Číslo $\lambda \in \mathbb{C}$ je vlastním číslem operátoru $x \in V_n$, právě když existuje nenulový vektor $x \in V_n$ splňující

$$Ax = \lambda x,$$

což je ovšem ekvivalentní podmínce vyjádřené pomocí souřadnic a matice operátoru následovně

$${}^{\mathcal{X}}A \cdot \lceil x \rceil_{\mathcal{X}} = \lambda \lceil x \rceil_{\mathcal{X}}.$$

[19] Toto je velmi netriviální krok! Viz Poznámku č. 7.24.

Celkem tedy platí následující tvrzení: λ je vlastní číslo operátoru A a $x \in V_n$ je jemu příslušný vlastní vektor, *právě když* λ je vlastní číslo matice ${}^{\mathcal{X}}A$ s vlastním vektorem $\lceil x \rceil_{\mathcal{X}}$. V tomto smyslu jsou uvedené pojmy (vlastní čísla a vektory operátoru a zobrazení) ekvivalentní.

Spektrum operátoru a spektrum jeho matice v (libovolné) bázi $\mathcal{X}$ jsou proto shodné,

$$\sigma(A) = \sigma({}^{\mathcal{X}}A).$$

S vlastními vektory musíme být více opatrní, protože jak bylo popsáno v předchozím odstavci, do úvahy vstupují souřadnice. Zdůrazněme tento fakt znovu a podrobněji, máme-li matici operátoru A vzhledem k bázi $\mathcal{X}$, ozn. $\mathbb{A} = {}^{\mathcal{X}}A$, tak potom je-li $\lambda \in \mathbb{C}$ vlastní číslo matice $\mathbb{A}$ a $\mathbb{x}$ jemu příslušející vlastní vektor, pak λ je vlastní číslo operátoru A a jemu příslušejícím vlastním vektorem je vektor x mající souřadnice v bázi $\mathcal{X}$ dány rovností $\lceil x \rceil_{\mathcal{X}} = \mathbb{x}$.

Násobnosti vlastních čísel matic definujeme prakticky identicky jako v případě operátorů:

Definice 7.19. *Nechť $\lambda \in \mathbb{C}$ je vlastní číslo matice $\mathbb{A} \in \mathbb{C}^{n,n}$. Potom*

- ***algebraickou násobností vlastního čísla*** *λ, ozn. $\nu_a(\lambda)$, nazýváme jeho násobnost jakožto kořene charakteristického polynomu $p_{\mathbb{A}}$,*
- ***geometrickou násobností vlastního čísla*** *λ, ozn. $\nu_g(\lambda)$, nazýváme dimenzi podprostoru všech řešení homogenní soustavy $(\mathbb{A} - \lambda\mathbb{E}) \cdot \mathbb{x} = \theta$.*

Z toho, co bylo řečeno již dříve o vlastních číslech a vektorech operátorů, nyní ihned plyne následující postup pro hledání vlastních čísel a vektorů matic. Skutečně, stačí si vlastně na místě matice $\mathbb{A}$ představit matici jistého operátoru v jisté bázi.

Algoritmus 7.20 (Výpočet vlastních čísel matice $\mathbb{A}$ a jejich algebraických násobností)**.** *Mějme matici $\mathbb{A} \in \mathbb{C}^{n,n}$.*

1. *Spočtěme charakteristický polynom matice $\mathbb{A}$, $p_{\mathbb{A}}(\lambda) = \det(\mathbb{A} - \lambda\mathbb{E})$, pomocí známých metod pro výpočet determinantu (Kapitola č. 6).*
2. *Nalezněme všechny kořeny polynomu $p_{\mathbb{A}}$. Tyto kořeny jsou vlastní čísla operátoru $\mathbb{A}$.*
3. *Algebraická násobnost vlastního čísla λ, tj. $\nu_a(\lambda)$, je násobnost λ jako kořene charakteristického polynomu $p_{\mathbb{A}}$.*

Algoritmus 7.21 (Výpočet vlastních vektorů matice $\mathbb{A}$ a geometrických násobností)**.** *Mějme matici $\mathbb{A} \in \mathbb{C}^{n,n}$ a její vlastní číslo $\lambda \in \mathbb{C}$.*

1. *Vlastní vektory příslušné vlastnímu číslu λ jsou všechna nenulová řešení homogenní rovnice $(\mathbb{A} - \lambda\mathbb{E}) \cdot \mathbb{x} = \theta$.*
2. *Geometrická násobnost vlastního čísla λ, tj. $\nu_g(\lambda)$, je dimenze podprostoru všech řešení homogenní rovnice $(\mathbb{A} - \lambda\mathbb{E}) \cdot \mathbb{x} = \theta$.*

Příklad 7.22. *Spočtěme vlastní čísla, obě jejich násobnosti, a k nim příslušející lineárně nezávislé vlastní vektory pro jednotkovou matici* $\mathbb{E} \in \mathbb{C}^{n,n}$.

Pro její charakteristický polynom platí

$$p_{\mathbb{E}}(\lambda) = \det(\mathbb{E} - \lambda\mathbb{E}) = (1 - \lambda)^n \det \mathbb{E} = (1 - \lambda)^n.$$

Tento polynom má právě jeden kořen $\lambda_1 = 1$ *s násobností* n. *Jediným vlastním číslem matice* $\mathbb{E}$ *je proto číslo* 1, $\sigma(\mathbb{E}) = \{1\}$, *a jeho algebraická násobnost je* n, $\nu_a(1) = n$. *Hledejme dále příslušné vlastní vektory. Je potřeba nalézt všechna řešení homogenní soustavy s maticí*

$$\mathbb{E} - 1 \cdot \mathbb{E} = \Theta.$$

Takovouto soustavu zřejmě řeší libovolný vektor z $\mathbb{C}^n$; $\dim \mathbb{C}^n = n$ *a číslo* 1 *má proto geometrickou násobnost* n, $\nu_g(1) = n$. *Například vektory standardní báze prostoru* $\mathbb{C}^n$ *tvoří* n *lineárně nezávislých vlastní vektorů příslušejících k vlastnímu číslu* 1.

Příklad 7.23. *Uvažme diagonální matici*

$$\mathbb{A} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}$$

a spočtěme její vlastní čísla a vlastní vektory.

Charakteristickým polynomem matice $\mathbb{A}$ *je zřejmě polynom*

$$p_{\mathbb{A}}(\lambda) = (1 - \lambda)^3 (2 - \lambda)^2 (3 - \lambda).$$

Proto $\sigma(\mathbb{A}) = \{1, 2, 3\}$. *Pro algebraické násobnosti platí*

$$\nu_a(1) = 3,\ \nu_a(2) = 2 \text{ a } \nu_a(3) = 1.$$

Za lineárně nezávislé vlastní vektory lze volit:

$$\begin{aligned} &\textit{pro vlastní číslo } 1: && e_1,\ e_2,\ e_3, \\ &\textit{pro vlastní číslo } 2: && e_4,\ e_5, \\ &\textit{pro vlastní číslo } 3: && e_6, \end{aligned}$$

kde e_j *označuje* j*tý vektor standardní báze* $\mathbb{C}^5$. *Pro geometrické násobnosti proto platí*

$$\nu_g(1) = 3,\ \nu_g(2) = 2 \text{ a } \nu_g(3) = 1.$$

Poznámka 7.24 (Matice společnice)**.** *V textu výše jsme popsali jak hledat vlastní čísla matic a operátorů pomocí hledání kořenů komplexních polynomů. To ovšem samo o sobě není jednoduchá úloha. Představte si, že máte matici relativně malého*[20] *rozměru* $\mathbb{A} \in \mathbb{C}^{100,100}$. *Její charakteristický polynom má stupeň* 100. *Najděte jeho kořeny. . .*

[20] V aplikacích se objevují i matice řádově vyšších rozměrů.

Existuje nějaký efektivní způsob (skutečný algoritmus – ne středoškolské hádání kořenů a vytýkání kořenových činitelů) jak hledat kořeny komplexních polynomů? Odpověď na tuto otázku je pozitivní a na první pohled lehce paradoxní[21].

Mějme komplexní polynom p stupně $n \in \mathbb{N}$ daný předpisem

$$p(\lambda) = \sum_{k=0}^{n} a_k \lambda^k$$

jehož kořeny chceme najít. Bez újmy na obecnosti lze[22] *předpokládat, že $a_n = 1$. Sestrojme tzv. matici společnici*[23] *$\mathbb{A}_p$ polynomu p:*

$$\mathbb{A}_p = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

Charakteristický polynom této matice je přesně polynom p! Skutečně, necháme čtenáři na rozmyšlení, že pokud při výpočtu následujícího determinantu

$$p_{\mathbb{A}_p}(\lambda) = \det(\mathbb{A}_p - \lambda\mathbb{E}) = \begin{vmatrix} -\lambda & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & -\lambda & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & -\lambda & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -\lambda & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} - \lambda \end{vmatrix}_{n \times n}$$

použije rozvoj podle posledního sloupce, dostane právě

$$p_{\mathbb{A}_p}(\lambda) = a_0 + a_1\lambda + \cdots + a_{n-1}\lambda^{n-1} + \lambda^n = p(\lambda).$$

Jinak řečeno, kořeny zadaného polynomu p jsou právě vlastní čísla matice společnice $\mathbb{A}_p$.

Pokud bychom tedy měli algoritmus počítající vlastní čísla matic nějakým alternativním způsobem (tj. ne pomocí hledání kořenů polynomů), tak tento algoritmus můžeme použít i na hledání kořenů libovolného komplexního (samozřejmě i reálného) polynomu. Takové numerické algoritmy skutečně existují, jako jeden příklad zmiňme QR algoritmus. Popis tohoto algoritmu je ovšem mimo možnosti tohoto úvodního textu a na tomto místě se spokojíme pouze s touto poznámkou.

Podobné matice

V případě lineárních operátorů jsme měli možnost volby báze, vůči které poté počítáme matici daného operátoru. Pro různé báze můžeme pro stejný operátor dostat

[21] *Plot twist!*
[22] Dle předpokladu je určitě $a_n \neq 0$ a my řešíme rovnici $p(\lambda) = 0$ což je ekvivalentní $\frac{1}{a_n} p(\lambda) = 0$.
[23] *Companion matrix.*

různé matice[24]. V případě, že máme dvě matice $\mathbb{A}$ a $\mathbb{B}$ z $\mathbb{C}^{n,n}$ tak má smysl se ptát, jestli náhodou nejde o matice jednoho operátoru, jen v různých bázích. Takovéto matice pak budou mít automaticky stejné spektrum. Zavádíme proto následující pojem.

Definice 7.25. *Matice $\mathbb{A}, \mathbb{B} \in \mathbb{C}^{n,n}$ nazveme **podobné**, právě když existuje regulární matice $\mathbb{P} \in \mathbb{C}^{n,n}$ taková, že platí*

$$\mathbb{A} = \mathbb{P}^{-1} \cdot \mathbb{B} \cdot \mathbb{P}.$$

Při ověřování podobnosti dvou matic $\mathbb{A}$ a $\mathbb{B}$ přímo podle definice si je dobré uvědomit, že rovnost $\mathbb{A} = \mathbb{P}^{-1} \cdot \mathbb{B} \cdot \mathbb{P}$ pro regulární matici $\mathbb{P}$ je ekvivalentní rovnosti $\mathbb{P} \cdot \mathbb{A} = \mathbb{B} \cdot \mathbb{P}$. Vyhneme se tím nutnosti invertovat matici $\mathbb{P}$.

Snadno lze dokázat, že relace podobnosti na množině všech matic z $\mathbb{C}^{n,n}$ je relace ekvivalence, proto důkaz následující věty necháváme na rozmyšlení laskavému čtenáři. Jediné co stačí využít je definice podobnosti a základní vlastnosti práce s maticovým násobením.

Věta 7.26. *Relace podobnosti zavedená v Definici č. 7.25 je relace ekvivalence[25], což znamená, že pro libovolné tři matice $\mathbb{A}, \mathbb{B}, \mathbb{D} \in \mathbb{C}^{n,n}$ platí následující tvrzení:*

1. *$\mathbb{A}$ je podobná $\mathbb{A}$,*
2. *pokud $\mathbb{A}$ je podobná $\mathbb{B}$, pak $\mathbb{B}$ je podobná $\mathbb{A}$,*
3. *pokud $\mathbb{A}$ je podobná $\mathbb{B}$ a $\mathbb{B}$ je podobná $\mathbb{D}$, pak $\mathbb{A}$ je podobná $\mathbb{D}$.*

Tento vztah podobnosti matic přesně vystihuje to, co jsme zmiňovali v úvodním odstavci této podkapitoly. Skutečně, platí totiž následující věta.

Věta 7.27. *Nechť $\mathbb{A}, \mathbb{B} \in \mathbb{C}^{n,n}$. Potom $\mathbb{A}$ je podobná $\mathbb{B}$ právě tehdy, když existuje operátor $A \in \mathcal{L}(\mathbb{C}^n)$ a dvě báze $\mathcal{X}$ a $\mathcal{Y}$ prostoru $\mathbb{C}^n$ takové, že*

$${}^{\mathcal{X}}A = \mathbb{A} \quad a \quad {}^{\mathcal{Y}}A = \mathbb{B}.$$

Důkaz. $\Rightarrow$: Nechť $\mathbb{A}$ a $\mathbb{B}$ jsou podobné, tedy existuje regulární matice $\mathbb{P}$ splňující

$$\mathbb{A} = \mathbb{P}^{-1} \cdot \mathbb{B} \cdot \mathbb{P}. \tag{7.4}$$

Na prostoru $\mathbb{C}^n$ definujme lineární operátor $A \in \mathcal{L}(\mathbb{C}^n)$ předpisem

$$Ax := \mathbb{A} \cdot x, \quad x \in \mathbb{C}^n.$$

Pro matici tohoto operátoru ve standardní bázi $\mathcal{X} := \mathcal{E}_n$ jistě platí

$${}^{\mathcal{X}}A = \mathbb{A}.$$

[24] Výjimkou je například identický operátor.

[25] S tímto pojmem (relace ekvivalence) se podrobněji setkáte v zimním semestru druhého ročníku v předmětu Základy diskrétní matematiky (BI-ZDM).

Matice $\mathbb{P}^{-1}$ je regulární, a proto její sloupce (ozn. $y_j := (\mathbb{P}^{-1}_{:j})^T \in \mathbb{C}^n$, $j \in \hat{n}$) tvoří soubor n lineárně nezávislých vektorů a tedy i bázi $\mathcal{Y} = (y_1, \ldots, y_n)$ prostoru $\mathbb{C}^n$. Platí tedy

$$\mathbb{P}^{-1} = {}^{\mathcal{Y}}E^{\mathcal{X}} \quad \text{a} \quad \mathbb{P} = {}^{\mathcal{X}}E^{\mathcal{Y}}.$$

Úpravou vztahu (7.4) nyní s pomocí Věty č. 5.39 dostáváme

$$\mathbb{B} = \mathbb{P} \cdot \mathbb{A} \cdot \mathbb{P}^{-1} = {}^{\mathcal{X}}E^{\mathcal{Y}} \cdot {}^{\mathcal{X}}A \cdot {}^{\mathcal{Y}}E^{\mathcal{X}} = {}^{\mathcal{Y}}A.$$

$\Leftarrow$: Mějme operátor $A \in \mathcal{L}(\mathbb{C}^n)$ a dvě báze $\mathcal{X}$ a $\mathcal{Y}$ prostoru $\mathbb{C}^n$ pro které platí

$$\mathbb{A} = {}^{\mathcal{X}}A \quad \text{a} \quad \mathbb{B} = {}^{\mathcal{Y}}A.$$

Potom podle Věty č. 5.39 platí

$$\mathbb{A} = {}^{\mathcal{X}}A = {}^{\mathcal{X}}A^{\mathcal{X}} = {}^{\mathcal{Y}}E^{\mathcal{X}} \cdot {}^{\mathcal{Y}}A^{\mathcal{Y}} \cdot {}^{\mathcal{X}}E^{\mathcal{Y}} = \mathbb{P}^{-1} \cdot \mathbb{B} \cdot \mathbb{P},$$

kde jsme označili $\mathbb{P} = {}^{\mathcal{X}}E^{\mathcal{Y}}$. Matice $\mathbb{P}$, jakožto matice přechodu, je regulární. □

Podobné matice mají i „podobné“ vlastnosti. Například mají stejné spektrum. Naopak tedy platí, že pokud matice $\mathbb{A}$ a $\mathbb{B}$ *nemají* stejné spektrum, tak *nejsou* podobné.

Věta 7.28. *Mějme dvě podobné matice $\mathbb{A}, \mathbb{B} \in \mathbb{C}^{n,n}$. Potom platí následující tvrzení.*

1. *Charakteristické polynomy obou matic jsou shodné, tj. $p_{\mathbb{A}} = p_{\mathbb{B}}$.*

2. *Spektra obou matic jsou stejná, tj. $\sigma(\mathbb{A}) = \sigma(\mathbb{B})$.*

Důkaz. Dle Věty č. 7.27 pro podobné matice $\mathbb{A}$ a $\mathbb{B}$ existuje operátor $A \in \mathcal{L}(\mathbb{C}^n)$ a dvě báze $\mathcal{X}$ a $\mathcal{Y}$ prostoru $\mathbb{C}^n$ splňující $\mathbb{A} = {}^{\mathcal{X}}A$ a $\mathbb{B} = {}^{\mathcal{Y}}A$. Dále z Lemmatu č. 7.6 pro charakteristické polynomy matic a operátoru platí

$$p_{\mathbb{A}}(\lambda) = p_{{}^{\mathcal{X}}A}(\lambda) = p_{{}^{\mathcal{Y}}A}(\lambda) = p_{\mathbb{B}}(\lambda)$$

pro každé $\lambda \in \mathbb{C}$. Charakteristické polynomy matic $\mathbb{A}$ a $\mathbb{B}$ jsou stejné a mají proto i stejné kořeny. Tyto kořeny tvoří spektra příslušných matic, a proto jsou i spektra matice $\mathbb{A}$ a $\mathbb{B}$ shodná. □

Příklad 7.29. *Pokud dvě matice* mají *stejné spektrum, tak z toho ještě neplyne, že jsou podobné. Jako příklad vezměme matice*

$$\mathbb{A} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad a \quad \mathbb{B} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

a pokusme se o jejich podobnosti rozhodnout z definice. Poznamenejme, že pro obě matice platí $\sigma(\mathbb{A}) = \sigma(B) = \{1\}$.

Hledáme regulární matici

$$\mathbb{P} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

splňující $\mathbb{P} \cdot \mathbb{A} = \mathbb{B} \cdot \mathbb{P}$, *tj.*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}.$$

Tato rovnost rozepsána po složkách představuje soustavu čtyř rovnic pro čtyři neznámé, která po jednoduché úpravě a vypuštění lineárně závislých rovnic má tvar

$$c = 0, \quad d = 0.$$

Ačkoliv a *a* b *mohou být libovolná, tak naše matice* $\mathbb{P}$ *musí mít nulový druhý řádek a nikdy nemůže být regulární. Neexistuje proto regulární matice* $\mathbb{P}$*, která by zajišťovala podobnost matic* $\mathbb{A}$ *a* $\mathbb{B}$*. Tyto dvě matice nejsou podobné, i když mají stejné spektrum*[26]*.*

Příklad 7.30. *Rozhodněme o podobnosti matic*

$$A = \begin{pmatrix} 87 & 510 \\ -15 & -88 \end{pmatrix} \quad B = \begin{pmatrix} 452 & -1950 \\ 105 & -453 \end{pmatrix}.$$

Pokusme ověřit přímo podmínku z definice podobnosti (Definice č. 7.25). Tato podmínka je ekvivalentní existenci regulární matice $\mathbb{P}$ *splňující*

$$\mathbb{P} \cdot \mathbb{A} = \mathbb{B} \cdot \mathbb{P}. \tag{7.5}$$

Označme prvky zatím neznámé matice následovně

$$\mathbb{P} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Potom je požadavek (7.5) ekvivalentní soustavě čtyř lineárních rovnic pro čtyři neznámé

$$\begin{aligned} -365a - 15b + 1950c &= 0, \\ 510a - 540b + 1950d &= 0, \\ -105a + 540c - 15d &= 0, \\ -105b + 510c + 365d &= 0. \end{aligned}$$

Matici této homogenní soustavy snadno převedeme do horního stupňovitého tvaru pomocí ekvivalentních úprav GEM. Dostáváme (pořadí sloupců odpovídá abecednímu pořadí proměnných)

$$\begin{pmatrix} 21 & 0 & -108 & 3 \\ 0 & 21 & -102 & -73 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

[26] Vnímavý čtenář si jistě povšimne, že jejich společné vlastní číslo 1 má u obou matic algebraickou násobnost 2, ale liší se v geometrické násobnosti (pro A je tato rovna 2 a v případě $\mathbb{B}$ pouze 1).

Tato soustava má nekonečně mnoho řešení, odpovídá některé z nich regulární matici $\mathbb{P}$? Zkusme zvolit například

$$a = 390,\ b = 0,\ c = 73,\ d = -102.$$

Tj.

$$\mathbb{P} = \begin{pmatrix} 390 & 0 \\ 73 & -102 \end{pmatrix}.$$

Tato matice je jistě regulární ($\det \mathbb{P} = -39\,780$) *a z její konstrukce a priori víme, že splňuje*

$$\mathbb{P} \cdot \mathbb{A} = \mathbb{B} \cdot \mathbb{P}.$$

Matice $\mathbb{A}$ a $\mathbb{B}$ jsou proto podobné. Uvedený postup jistě můžeme aplikovat i na matice větších rozměrů. Budeme-li rozhodovat o podobnosti matic $\mathbb{A}, \mathbb{B} \in \mathbb{C}^{n,n}$, budeme muset řešit soustavu n^2 rovnic pro n^2 neznámých. To nemusí být vždy příjemné. V Příkladu č. 7.39 si ukážeme alternativní postup využívající diagonalizace.

7.4 Diagonalizace lineárního operátoru a matice

Jak jsme již naznačili, pro některé operátory je možné najít bázi, v níž je matice daného operátoru diagonální. Analogický pojem přirozeně opět máme i pro matice.

Definice 7.31. *Operátor $A \in \mathcal{L}(V_n)$ nazveme **diagonalizovatelný**, jestliže existuje báze $\mathcal{X}$ prostoru V_n taková, že matice ${}^{\mathcal{X}}\!A$ je diagonální. Matici $\mathbb{A} \in \mathbb{C}^{n,n}$ nazveme **diagonalizovatelnou**, jestliže je podobná diagonální matici.*

Za jakých předpokladů je možné operátor A diagonalizovat? Nejprve dokažme pomocné tvrzení.

Lemma 7.32. *Nechť $A \in \mathcal{L}(V)$ a $\lambda_1, \ldots, \lambda_k$ jsou navzájem různá vlastní čísla operátoru A, a nechť pro každé $i \in \hat{k}$ označuje x_i vlastní vektor A příslušející vlastnímu číslu λ_i. Potom je soubor $(x_1, \ldots, x_k)$ LN.*

Důkaz. Důkaz provedeme indukcí podle délky souboru.

- Každý vlastní vektor je nenulový, a proto je soubor (x_1) LN.
- Mějme $j \in \{1, 2, \ldots, k-1\}$ a předpokládejme lineární nezávislost souboru $(x_1, x_2, \ldots, x_j)$. Ukážeme, že i soubor $(x_1, x_2, \ldots, x_j, x_{j+1})$ je LN a to sporem. Kdyby byl LZ, tak lze jeho poslední vektor (tj. x_{j+1}) vyjádřit pomocí vektorů předchozích. Existovaly by tedy konstanty $\alpha_1, \ldots, \alpha_j \in \mathbb{C}$ splňující

  $$x_{j+1} = \sum_{i=1}^{j} \alpha_i x_i.$$

  Navíc alespoň jedna z těchto konstant, např. α_{j^*}, by byla nenulová, protože vektor x_{j+1} je jakožto vlastní vektor nutně nenulový. Aplikujeme-li na obě strany operátor A dostaneme s využitím jeho linearity rovnost

  $$Ax_{j+1} = A\left(\sum_{i=1}^{j} \alpha_i x_i\right) = \sum_{i=1}^{j} \alpha_i A x_i.$$

Nyní si stačí vzpomenout, jak působí operátor A na svých vlastních vektorech, čímž dostaneme

$$\lambda_{j+1} x_{j+1} = \sum_{i=1}^{j} \alpha_i \lambda_i x_i. \tag{7.6}$$

Na druhou stranu ovšem triviálně platí

$$\lambda_{j+1} x_{j+1} = \lambda_{j+1} \sum_{i=1}^{j} \alpha_i x_i = \sum_{i=1}^{j} \alpha_i \lambda_{j+1} x_i. \tag{7.7}$$

Odečtením rovnice (7.7) od (7.6) dostaneme rovnost

$$\theta = \sum_{i=1}^{j} (\lambda_i - \lambda_{j+1}) \alpha_i x_i.$$

Koeficient $(\lambda_{j^*} - \lambda_{j+1})\alpha_{j^*}$ je ale určitě nenulový (vlastní čísla jsou vzájemně různá a o čísle α_{j*} víme, že je nenulové). To je ovšem spor s lineární nezávislostí souboru $(x_1, \dots, x_j)$. □

Následující věta nejen dává nutnou a postačující podmínku diagonalizovatelnosti operátoru, ale její důkaz[27] i ukazuje jak pak zkonstruovat bázi, vůči níž je daný operátor diagonální.

Věta 7.33 (O diagonalizovatelnosti). *Operátor $A \in \mathcal{L}(V_n)$ je diagonalizovatelný, právě když každé z vlastních čísel λ operátoru A má stejnou algebraickou a geometrickou násobnost, tj.*

$$(\forall \lambda \in \sigma(A))(\nu_a(\lambda) = \nu_g(\lambda)).$$

Důkaz. $\Rightarrow$: Předpokládejme, že operátor $A \in \mathcal{L}(V_n)$ je diagonalizovatelný. Existuje tedy báze $\mathcal{X}$ prostoru V_n vůči níž má operátor A diagonální matici v blokovém tvaru

$$^{\mathcal{X}}A = \begin{pmatrix} \lambda_1 \mathbb{E}_{\ell_1} & \Theta & \Theta & \cdots & \Theta \\ \Theta & \lambda_2 \mathbb{E}_{\ell_2} & \Theta & \cdots & \Theta \\ \Theta & \Theta & \lambda_3 \mathbb{E}_{\ell_3} & \cdots & \Theta \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \Theta & \Theta & \Theta & \cdots & \lambda_k \mathbb{E}_{\ell_k} \end{pmatrix}$$

kde $k \in \hat{n}$, $\lambda_1, \dots, \lambda_k \in \mathbb{C}$ jsou vzájemně různá čísla a $\mathbb{E}_{\ell_j}$ jsou jednotkové matice rozměru $\ell_j \times \ell_j$, $j \in \hat{k}$, a konečně Θ jsou nulové matice různých rozměrů. Opravdu, jednoduchou změnou pořadí bazických vektorů báze $\mathcal{X}$ můžeme docílit, že stejná čísla na diagonále $^{\mathcal{X}}A$ jsou takto vedle sebe. Odtud ale ihned plyne, že charakteristický polynom operátoru A je

$$p_A(\lambda) = \det {}^{\mathcal{X}}(A - \lambda E) = \prod_{j=1}^{k} (\lambda_j - \lambda)^{\ell_j}$$

a čísla $\lambda_1, \dots, \lambda_k$ jsou právě vlastní čísla operátoru A. Jejich algebraické násobnosti jsou popořadě $\ell_1, \dots, \ell_k$. Konečně i jejich geometrické násobnosti jsou popořadě

[27] Studujte důkazy!

rovny $\ell_1, \ldots, \ell_k$. Skutečně, k vlastnímu číslu λ_1 existuje ℓ_1 LN vlastních vektorů – je jimi přímo prvních ℓ_1 vektorů báze $\mathcal{X}$. Podobně pro další vlastní čísla. Ověřili jsme tedy platnost vztahu $\nu_a(\lambda) = \nu_g(\lambda)$ pro libovolné $\lambda \in \sigma(A)$.

$\Leftarrow$: Nyní naopak předpokládejme, že operátor $A \in \mathcal{L}(V_n)$ má právě $k \in \hat{n}$ vzájemně různých vlastních čísel $\lambda_1, \ldots, \lambda_k \in \mathbb{C}$ jejichž algebraické a geometrické násobnosti pro každé $j \in \hat{k}$ splňují

$$\nu_a(\lambda_j) = \nu_g(\lambda_j) =: \ell_j.$$

Označme dále $x_{j,\ell} \in V_n$, $j \in \hat{k}$, $\ell \in \hat{\ell}_j$ lineárně nezávislé vlastní vektory příslušející vlastnímu číslu λ_j. To jistě lze, protože vlastní podprostor $\ker(A - \lambda_j E)$ má dimenzi ℓ_j, a proto v něm lze nalézt ℓ_j lineárně nezávislých vlastních vektorů $x_{j,1}, \ldots, x_{j,\ell_j}$.

Sestavme soubor

$$\mathcal{X} = (x_{1,1}, \ldots, x_{1,\ell_1}, x_{2,1}, \ldots, x_{2,\ell_2}, \ldots, x_{k,1}, \ldots, x_{k,\ell_k}).$$

Tvoří tento soubor bázi prostoru V_n? Jelikož ℓ_j jsou rovny algebraickým násobnostem vlastních čísel λ_j, plyne z vlastností kořenů polynomu p_A rovnost $\ell_1 + \ell_2 + \cdots + \ell_k = n$, tedy soubor $\mathcal{X}$ má „správný počet prvků“ a tvoří bázi V_n právě tehdy, když je LN. Ukažme nyní jeho lineární nezávislost. Uvažme proto lineární kombinaci souboru $\mathcal{X}$ dávající nulový vektor,

$$\sum_{j=1}^{k} \sum_{\ell=1}^{\ell_j} \alpha_{j,\ell} x_{j,\ell} = \theta. \tag{7.8}$$

Označme

$$u_j := \sum_{\ell=1}^{\ell_j} \alpha_{j,\ell} x_{j,\ell}.$$

Tvrdíme, že $u_j = \theta$ pro každé $j \in \hat{k}$. Skutečně, u_j totiž patří do vlastního podprostoru $\ker(A - \lambda_j E)$ a je-li nenulový, pak je vlastním vektorem operátoru A příslušejícím vlastnímu číslu λ_j. Rovnost (7.8) by proto představovala netriviální lineární kombinaci těchto vektorů dávající nulový vektor,

$$\sum_{j=1}^{k} u_j = \theta.$$

O nenulových vlastních vektorech příslušejících různým vlastním číslům ale dle Lemmatu č. 7.32 víme, že tvoří lineárně nezávislý soubor. Ani jeden z vektorů u_j proto nemůže být nenulový. Celkem jsme tedy pro každé $j \in \hat{k}$ odvodili rovnost

$$u_j = \sum_{\ell=1}^{\ell_j} \alpha_{j,\ell} x_{j,\ell} = \theta$$

a z lineární nezávislosti souboru[28] $(x_{j,1}, \ldots, x_{j,\ell_j})$ plynou rovnosti

$$\alpha_{j,1} = \alpha_{j,2} = \cdots = \alpha_{j,\ell_j} = 0$$

[28]Tak jsme tento soubor konstruovali.

pro každé $j \in \hat{k}$.

Protože z definice vektorů $x_{j,\ell}$ plyne rovnost $Ax_{j,\ell} = \lambda_j x_{j,\ell}$ je matice A vzhledem k bázi $\mathcal{X}$ rovna

$$^{\mathcal{X}}A = \begin{pmatrix} \lambda_1 \mathbb{E}_{\ell_1} & \Theta & \Theta & \cdots & \Theta \\ \Theta & \lambda_2 \mathbb{E}_{\ell_2} & \Theta & \cdots & \Theta \\ \Theta & \Theta & \lambda_3 \mathbb{E}_{\ell_3} & \cdots & \Theta \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \Theta & \Theta & \Theta & \cdots & \lambda_k \mathbb{E}_{\ell_k} \end{pmatrix}$$

a je tedy diagonální. $\square$

Důsledek 7.34. *Nechť $A \in \mathcal{L}(V_n)$ a $(\forall \lambda \in \sigma(A))(\nu_a(\lambda) = 1)$, potom je A diagonalizovatelný.*

Důkaz. Vzpomeňte si na vztah mezi násobnostmi. Geometrická násobnost vlastního čísla λ splňuje $1 \leq \nu_g(\lambda) \leq \nu_a(\lambda)$. Proto v uvažovaném případě platí $\nu_g(\lambda) = \nu_a(\lambda) = 1$. $\square$

Shrňme si v následující poznámce jak diagonalizovat diagonalizovatelný operátor. Stačí jen extrahovat postup z druhé části důkazu Věty č. 7.33.

Poznámka 7.35 (Diagonalizace operátoru)**.** *Mějme operátor $A \in \mathcal{L}(V_n)$ s vlastními čísly $\lambda_1, \ldots, \lambda_k$ (kde $k \in \hat{n}$) s násobnostmi $\ell_j = \nu_a(\lambda_j) = \nu_g(\lambda_j)$ pro každé $j \in \hat{k}$. Ke každému vlastnímu číslu λ_j ($j \in \hat{k}$) přísluší LN soubor vlastních vektorů, ten označme stejně jako dříve $(x_{j,1}, x_{j,2}, \ldots, x_{j,\ell_j})$. Potom vzhledem k bázi*

$$\mathcal{X} = (x_{1,1}, \ldots, x_{1,\ell_1}, x_{2,1}, \ldots, x_{2,\ell_2}, \ldots, x_{k,1}, \ldots, x_{k,\ell_k})$$

má operátor A matici zobrazení v diagonálním tvaru

$$^{\mathcal{X}}A = \begin{pmatrix} \lambda_1 \mathbb{E}_{\ell_1} & \Theta & \Theta & \cdots & \Theta \\ \Theta & \lambda_2 \mathbb{E}_{\ell_2} & \Theta & \cdots & \Theta \\ \Theta & \Theta & \lambda_3 \mathbb{E}_{\ell_3} & \cdots & \Theta \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \Theta & \Theta & \Theta & \cdots & \lambda_k \mathbb{E}_{\ell_k} \end{pmatrix}.$$

Jinak řečeno, sestavíme-li bázi tvořenou vlastními vektory operátoru A (to nelze vždy, viz podmínku diagonalizovatelnosti), pak matice operátoru A vzhledem k této bázi je diagonální a na diagonále má vlastní čísla operátoru A. Navíc pořadí vlastních čísel na diagonále odpovídá pořadí příslušných vektorů v této bázi. Vlastní číslo se na diagonále matice $^{\mathcal{X}}A$ opakuje tolikrát, kolik je jeho algebraická násobnost.

Tento postup můžeme přirozeně aplikovat i na problém diagonalizace matice.

Poznámka 7.36 (Diagonalizace matice)**.** *Mějme matici $\mathbb{A} \in \mathbb{C}^{n,n}$ s vlastními čísly $\lambda_1, \ldots, \lambda_k$, kde $k \in \hat{n}$, násobnostmi $\ell_j = \nu_a(\lambda_j) = \nu_g(\lambda_j)$ pro každé $j \in \hat{k}$. Označme příslušné lineárně nezávislé vlastní vektory $\mathbb{x}_{j,\ell} \in \mathbb{C}^n$, $\ell \in \hat{\ell_j}$ a $j \in \hat{k}$.*

Můžeme zavést operátor A, který na prostoru $\mathbb{C}^n$ působí dle předpisu

$$Ax = \mathbb{A} \cdot x, \quad x \in \mathbb{C}^n.$$

Odtud ihned plyne, že matice A vzhledem ke standardní bázi $\mathcal{E}$ prostoru $\mathbb{C}^n$ je právě matice $\mathbb{A}$, tj. ${}^{\mathcal{E}}A = \mathbb{A}$. Nyní můžeme postupovat dle předchozí poznámky. Utvoříme bázi $\mathbb{C}^n$ tvořenou vlastními vektory operátoru A,

$$\mathcal{X} = (\mathbb{x}_{1,1}, \ldots, \mathbb{x}_{1,\ell_1}, \mathbb{x}_{2,1}, \ldots, \mathbb{x}_{2,\ell_2}, \ldots, \mathbb{x}_{k,1}, \ldots, \mathbb{x}_{k,\ell_k})$$

Již víme, že vzhledem k této bázi má operátor diagonální matici zobrazení, ozn. $\mathbb{B} := {}^{\mathcal{X}}A$. Dále víme, že

$$\mathbb{B} = {}^{\mathcal{X}}A = {}^{\mathcal{E}}E^{\mathcal{X}} \cdot {}^{\mathcal{E}}A \cdot {}^{\mathcal{X}}E^{\mathcal{E}} = {}^{\mathcal{E}}E^{\mathcal{X}} \cdot \mathbb{A} \cdot {}^{\mathcal{X}}E^{\mathcal{E}}.$$

Označíme-li konečně $\mathbb{P} := {}^{\mathcal{X}}E^{\mathcal{E}}$ pak $\mathbb{B} = \mathbb{P}^{-1} \cdot \mathbb{A} \cdot \mathbb{P}$. Matice $\mathbb{A}$ je tedy podobná diagonální matici $\mathbb{B}$ a regulární matice $\mathbb{P}$ zaručující podobnost je právě matice přechodu z báze $\mathcal{X}$ do $\mathcal{E}$. Je to tedy matice, která má ve sloupcích popořadě vlastní vektory matice $\mathbb{A}$,

$$\mathbb{P} = \begin{pmatrix} \mathbb{x}_{1,1}^T & \cdots & \mathbb{x}_{1,\ell_1}^T & \mathbb{x}_{2,1}^T & \cdots & \mathbb{x}_{2,\ell_2}^T & \cdots & \mathbb{x}_{k,1}^T & \cdots & \mathbb{x}_{k,\ell_k}^T \end{pmatrix}.$$

Příklad 7.37. *Rozhodněte o diagonalizovatelnosti matice*

$$\mathbb{A} = \begin{pmatrix} -6 & -10 & 34 \\ 18 & 22 & -64 \\ 3 & 5 & -17 \end{pmatrix}.$$

Pokud je diagonalizovatelná zkonstruujte matici $\mathbb{P}$ převádějící ji na diagonální tvar.

Nejprve spočtěme charakteristický polynom

$$p_{\mathbb{A}}(\lambda) = \begin{vmatrix} -6-\lambda & -10 & 34 \\ 18 & 22-\lambda & -64 \\ 3 & 5 & -17-\lambda \end{vmatrix} = \begin{vmatrix} -6-\lambda & -10 & 34 \\ 0 & -8-\lambda & 38+6\lambda \\ 3 & 5 & -17-\lambda \end{vmatrix} =$$
$$= \frac{1}{3}\begin{vmatrix} 0 & 5\lambda & -\lambda^2-23\lambda \\ 0 & -8-\lambda & 38+6\lambda \\ 3 & 5 & -17-\lambda \end{vmatrix} = \lambda \begin{vmatrix} 5 & -\lambda-23 \\ -8-\lambda & 38+6\lambda \end{vmatrix} =$$
$$= \lambda(-\lambda^2 - \lambda + 6) = -\lambda(\lambda+3)(\lambda-2).$$

Vlastními čísly matice $\mathbb{A}$ proto jsou $\lambda_1 = 0$, $\lambda_2 = 2$ a $\lambda_3 = -3$. Každé z nich má algebraickou násobnost rovnou 1 a matice $\mathbb{A}$ je proto diagonalizovatelná (viz Důsledek č. 7.34).

Nyní musíme najít příslušné vlastní vektory, tj. nalézt nenulová řešení homogenních soustav $(\mathbb{A} - \lambda_i \mathbb{E}) \cdot \mathbb{x} = \theta$ pro $j = 1, 2, 3$. Uvedeme jen stručně výsledek[29]

$$\begin{aligned} \textit{pro } \lambda_1 = 0: &\quad (9, -19, -4), \\ \textit{pro } \lambda_2 = 2: &\quad (2, -5, -1), \\ \textit{pro } \lambda_3 = -3: &\quad (2, -4, -1). \end{aligned}$$

Matice $\mathbb{P}$, pro kterou platí

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -3 \end{pmatrix} = \mathbb{P}^{-1} \cdot \mathbb{A} \cdot \mathbb{P}$$

[29] Řešení soustav lineárních rovnic už máme touto dobou v malíčku.

proto je

$$\mathbb{P} = \begin{pmatrix} 9 & 2 & 2 \\ -19 & -5 & -4 \\ -4 & -1 & -1 \end{pmatrix}.$$

Příklad 7.38. *Rozhodněte o diagonalizovatelnosti matice*

$$\mathbb{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix}.$$

Abychom mohli využít Větu č. 7.33 musíme nalézt vlastní čísla matice $\mathbb{A}$ a jejich algebraické a geometrické násobnosti.

Charakteristickým polynomem matice $\mathbb{A}$ je polynom

$$p_{\mathbb{A}}(\lambda) = \begin{vmatrix} 1-\lambda & 0 & 0 \\ 0 & 3-\lambda & 1 \\ 0 & 0 & 3-\lambda \end{vmatrix} = (1-\lambda)(3-\lambda)^2.$$

Vlastními čísly matice $\mathbb{A}$ proto jsou komplexní čísla

$$\lambda_1 = 1 \ a \ \lambda_2 = 3.$$

Dále z faktorizace polynomu $p_{\mathbb{A}}$ vyčteme algebraické násobnosti těchto vlastních čísel,

$$\nu_a(1) = 1 \ a \ \nu_a(3) = 2.$$

Abychom nalezli jejich geometrické násobnosti, musíme prozkoumat příslušné vlastní podprostory. Vlastní vektory příslušné k vlastnímu číslu $\lambda_1 = 1$ jsou nenulová řešení homogenní soustavy s maticí

$$\mathbb{A} - \lambda_1\mathbb{E} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix},$$

tedy vektory $\langle(1,0,0)\rangle$. Za vlastní vektor příslušný k $\lambda_1 = 1$ tedy můžeme zvolit právě například $v_1 = (1,0,0)$. Geometrická násobnost $\lambda_1 = 1$ je proto rovna 1, $\nu_g(1) = 1$. V případě vlastního čísla $\lambda_2 = 3$ musíme podobně řešit soustavu

$$\mathbb{A} - \lambda_2\mathbb{E} = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Všechna její řešení očividně jsou $\langle(0,1,0)\rangle$. Za vlastní vektor příslušný k vlastnímu číslu $\lambda_2 = 3$ můžeme volit například $v_2 = (0,1,0)$. Konečně geometrická násobnost tohoto vlastního čísla je $\nu_g(3) = 1$.

Shrňme si, co jsme doposud spočítali. Matice $\mathbb{A}$ má vlastní čísla 1 a 3. Jejich násobnosti jsou

$$\nu_g(1) = \nu_a(1) = 1 \quad a \quad 1 = \nu_g(3) < \nu_a(3) = 2.$$

Matice $\mathbb{A}$ proto podle Věty č. 7.33 není diagonalizovatelná.

Příklad 7.39. *Pokusme se rozhodnout o podobnosti matic*

$$A = \begin{pmatrix} 87 & 510 \\ -15 & -88 \end{pmatrix} \quad a \quad B = \begin{pmatrix} 452 & -1950 \\ 105 & -453 \end{pmatrix}.$$

z Příkladu č. 7.30 rozhodnout pomocí diagonalizace.

Přímočarým výpočtem zjistíme, že charakteristické polynomy obou matic jsou shodné,

$$p_{\mathbb{A}}(\lambda) = p_{\mathbb{B}}(\lambda) = z^2 + z - 6 = (z+3)(z-2).$$

Obě proto mají stejné spektrum, $\sigma(\mathbb{A}) = \sigma(\mathbb{B}) = \{-3, 2\}$. Kdyby rovnost spekter neplatila, pak by $\mathbb{A}$ a $\mathbb{B}$ nebyly podobné[30]*. Spočtěme vlastní vektory, uvedeme jen stručně výsledky. Pro matici $\mathbb{A}$ jsou vlastními vektory*

$$\begin{aligned} \lambda_1 &= -3: & v_1 &= (17, -3), \\ \lambda_2 &= 2: & v_2 &= (6, -1), \end{aligned}$$

a pro matici $\mathbb{B}$ máme

$$\begin{aligned} \lambda_1 &= -3: & u_1 &= (30, 7), \\ \lambda_2 &= 2: & u_2 &= (13, 3). \end{aligned}$$

Algebraické i geometrické násobnosti jsou v obou případech shodné a obě matice jsou diagonalizovatelné. Z předchozího výkladu již víme jak obě matice diagonalizovat (pomocí vlastních vektorů):

$$\begin{pmatrix} -3 & 0 \\ 0 & 2 \end{pmatrix} = \mathbb{P}_{\mathbb{A}}^{-1} \cdot \mathbb{A} \cdot \mathbb{P}_{\mathbb{A}} = \mathbb{P}_{\mathbb{B}}^{-1} \cdot \mathbb{B} \cdot \mathbb{P}_{\mathbb{B}}, \tag{7.9}$$

kde matice $\mathbb{P}_{\mathbb{A}}$ a $\mathbb{P}_{\mathbb{B}}$ jsou sestavené pomocí vlastních vektorů (pozor na pořadí)

$$\mathbb{P}_{\mathbb{A}} = \begin{pmatrix} 17 & 6 \\ -3 & -1 \end{pmatrix} \quad a \quad \mathbb{P}_{\mathbb{B}} = \begin{pmatrix} 30 & 13 \\ 7 & 3 \end{pmatrix}.$$

Druhou rovnost z rovnice (7.9) lze ekvivalentně přepsat do tvaru (obě matice $\mathbb{P}_{\mathbb{A}}$ i $\mathbb{P}_{\mathbb{B}}$ jsou regulární)

$$\mathbb{A} = \left(\mathbb{P}_{\mathbb{B}} \cdot \mathbb{P}_{\mathbb{A}}^{-1}\right)^{-1} \cdot \mathbb{B} \cdot (\mathbb{P}_{\mathbb{B}} \cdot \mathbb{P}_{\mathbb{A}}^{-1}).$$

Matice zaručující podobnost matic $\mathbb{A}$ a $\mathbb{B}$ proto je

$$\mathbb{P} = \mathbb{P}_{\mathbb{B}} \cdot \mathbb{P}_{\mathbb{A}}^{-1} = \begin{pmatrix} 9 & 41 \\ 2 & 9 \end{pmatrix}.$$

Poznámka 7.40. *Pokud jsou dvě matice podobné stejné diagonální matici potom díky Větě č. 7.26 jsou si podobné navzájem. Naopak pokud matice $\mathbb{A}$ je podobná diagonální a $\mathbb{B}$ není podobná stejné diagonální matici (např. liší se spektrum, či násobnosti vlastních čísel), potom si nemůžou býti podobné.*

[30] Pokud matice nejsou podobné, pak tento postup bude pravděpodobně výrazně jednodušší než ověřování pomocí definice.

7.5 Příklady

V této kapitole ukážeme několik relativně jednoduchých aplikačních příkladů využívajících vlastní čísla a vlastní vektory. Při popisu problémů ovšem nebudeme zabíhat do detailů, příliš bychom tím opustili rámec tohoto textu.

Fibonacciho posloupnost

Čtenáři je jistě známa Fibonacciho posloupnost. Jde o reálnou číselnou posloupnost $(F_n)_{n=1}^{\infty}$, která je zadána rekurentně vztahem

$$F_n = F_{n-1} + F_{n-2}, \quad n = 3, 4, 5, \dots \tag{7.10}$$

a počátečními hodnotami $F_1 = F_2 = 1$. Pomocí těchto informací (rekurence a dvě počáteční hodnoty) jsme schopni vypočítat hodnotu F_n pro libovolné $n \in \mathbb{N}$. Prvních několik dalších členů této posloupnosti je

$$F_3 = 1 + 1 = 2, \quad F_4 = 2 + 1 = 3, \quad F_5 = 3 + 2 = 5.$$

Očividně se jedná o ostře rostoucí posloupnost celých čísel. Lze její členy vyjádřit explicitně? Tj. lze se zbavit rekurence? Lze říci, jak rychle Fibonacciho posloupnost roste do nekonečna[31]?

Klíčovým východiskem k zodpovězení těchto otázek je přeformulování rekurentního vztahu (7.10) do maticového tvaru. Utvořme sloupcový vektor $\mathbb{f}_n = \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix}$, $n = 2, 3, \dots$, nesoucí informaci o členech Fibbonaciho posloupnosti. Potom pro něj platí vektorový rekurentní vztah

$$\mathbb{f}_{n+1} = \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = \begin{pmatrix} F_n + F_{n-1} \\ F_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} = \mathbb{A} \cdot \mathbb{f}_n,$$

kde $n = 2, 3, 4, \dots$ a symbolem $\mathbb{A}$ jsme označili matici

$$\mathbb{A} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Dále platí $\mathbb{f}_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. K výpočtu vyšších a vyšších členů vektorové posloupnosti $(\mathbb{f}_n)_{n=2}^{\infty}$ tedy stačí počítat mocninu matice $\mathbb{A}$, konkrétně z výše uvedeného vektorového rekurentního vztahu plyne

$$\mathbb{f}_n = \mathbb{A}^{n-2} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad n = 2, 3, 4, \dots \tag{7.11}$$

Spočtěme **vlastní čísla** a vektory matice $\mathbb{A}$. Pro charakteristický polynom matice $\mathbb{A}$ platí

$$p_{\mathbb{A}}(\lambda) = \begin{vmatrix} 1-\lambda & 1 \\ 1 & -\lambda \end{vmatrix} = \lambda^2 - \lambda - 1.$$

[31] Vyzýváme čtenáře, aby na tomto místě zkusil zformulovat hypotézu o rychlosti růstu $(F_n)_{n=1}^{\infty}$. Roste polynomiálně, exponenciálně, jako faktoriál, nebo jinak?

Jeho kořeny jsou reálná čísla[32]

$$\lambda_\pm = \frac{1}{2}\left(1 \pm \sqrt{5}\right).$$

Vlastní vektor k $\lambda_\pm$ je libovolné nenulové řešení homogenní soustavy s maticí

$$\begin{pmatrix} 1-\lambda_\pm & 1 \\ 1 & -\lambda_\pm \end{pmatrix} \sim \begin{pmatrix} 1 & -\lambda_\pm \\ 0 & 0 \end{pmatrix}.$$

Zvolme například $v_\pm = (\lambda_\pm, 1)$.

Matice $\mathbb{A}$ je proto diagonalizovatelná, platí pro ni

$$\mathbb{P}^{-1} \cdot \mathbb{A} \cdot \mathbb{P} = \begin{pmatrix} \lambda_+ & 0 \\ 0 & \lambda_- \end{pmatrix},$$

kde

$$\mathbb{P} = (v_+^T \, v_-^T) = \begin{pmatrix} \lambda_+ & \lambda_- \\ 1 & 1 \end{pmatrix} \quad \text{a} \quad \mathbb{P}^{-1} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & -\lambda_- \\ -1 & \lambda_+ \end{pmatrix}.$$

Tudíž

$$\mathbb{A}^{n-2} = \mathbb{P} \cdot \begin{pmatrix} \lambda_+^{n-2} & 0 \\ 0 & \lambda_-^{n-2} \end{pmatrix} \cdot \mathbb{P}^{-1}.$$

Konečně dosazením tohoto vyjádření matice $\mathbb{A}$ do rovnice (7.11) dostáváme

$$\mathbb{f}_n = \mathbb{P} \cdot \begin{pmatrix} \lambda_+^{n-2} & 0 \\ 0 & \lambda_-^{n-2} \end{pmatrix} \cdot \mathbb{P}^{-1} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{5}} \mathbb{P} \cdot \begin{pmatrix} \lambda_+^{n-2} & 0 \\ 0 & \lambda_-^{n-2} \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 1-\lambda_- \\ \lambda_+ - 1 \end{pmatrix}}_{\begin{pmatrix} \lambda_+ \\ -\lambda_- \end{pmatrix}} =$$

$$= \frac{1}{\sqrt{5}} \mathbb{P} \cdot \begin{pmatrix} \lambda_+^{n-1} \\ -\lambda_-^{n-1} \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} \lambda_+^n - \lambda_-^n \\ \lambda_+^{n-1} - \lambda_-^{n-1} \end{pmatrix}.$$

Odtud ihned plyne kýžený vztah

$$F_n = \frac{1}{\sqrt{5}}\left(\lambda_+^n - \lambda_-^n\right). \tag{7.12}$$

Všimněme si, že

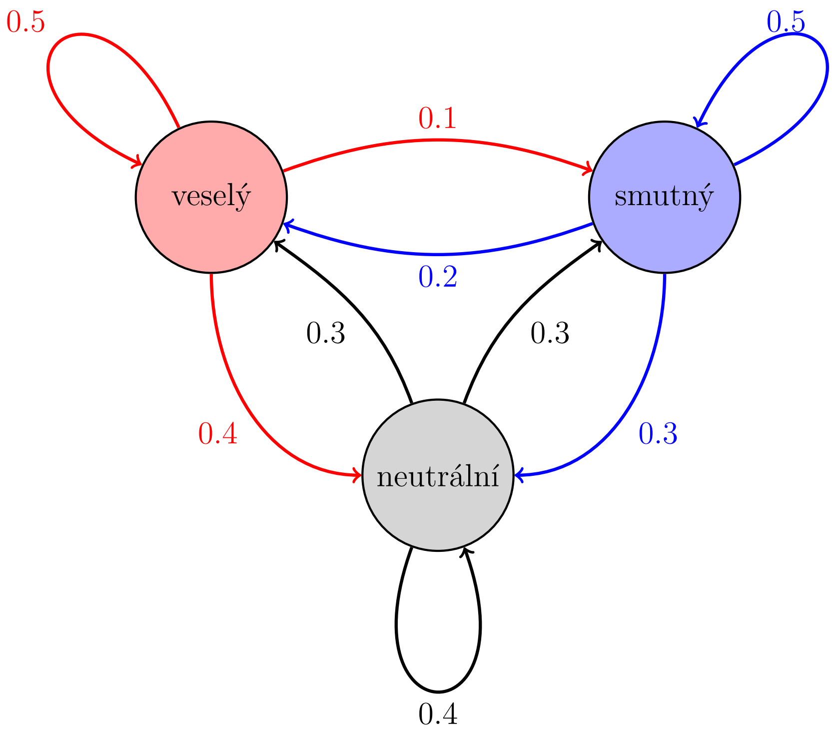
$$\lambda_+ \approx 1.61803398874989 \quad \text{a} \quad \lambda_- \approx -0.618033988749895.$$

Proto druhý člen v (7.12) s rostoucím n konverguje k nule a první člen naopak diverguje do nekonečna. Vidíme, že Fibbonacciho posloupnost je asymptoticky ekvivalentní geometrické posloupnosti s kvocientem λ_+ (zlatý řez), tj.

$$\lim_{n\to\infty} \frac{\frac{1}{\sqrt{5}}\lambda_+^n}{F_n} = 1.$$

Jinak řečeno, pro velká n se hodnota F_n přibližuje hodnotě $\frac{1}{\sqrt{5}}\lambda_+^n$. To je velmi netriviální tvrzení, které ze samotné definice Fibonacciho posloupnosti není na první pohled patrné.

[32] Číslo $\varphi = \frac{1+\sqrt{5}}{2}$ je známé pod názvem „zlatý řez“.



Obrázek 7.1: Denní mentální stavy Pepy Vomáčky a pravděpodobnosti přechodu mezi nimi.

Markovské řetězce

Uvažme systém, který se může nacházet v různých stavech a o němž víme, s jakou pravděpodobností může během jednoho časového kroku přecházet z jednoho stavu do jiného (uvažujeme diskrétní čas). O časovém vývoji takovéhoto systému pak mluvíme jako o (diskrétním) markovském řetězci[33]. Častým úkolem je pak zjistit pravděpodobnosti v jakém stavu se systém bude nacházet po nekonečném (velkém) počtu kroků. Tj. z popisu jeho krátkodobého chování chceme odvodit chování dlouhodobé.

V této podkapitole nebudeme zacházet příliš do detailů a k demonstraci takovéhoto systému použijeme jednoduše uchopitelný a představitelný příklad[34]. Uvažme Pepu Vomáčku, který je každý den buď veselý (V), smutný (S), nebo neutrální (N). Pravděpodobnosti, že následující den přejde z daného stavu do jiného stavu, nebo zůstane ve stejném stavu, byly odhadnuty jeho psychiatrem a jsou graficky znázorněny na Obrázku č. 7.1.

Označme si jednotlivé Pepovy nálady pomocí čísel: $V \leftrightarrow 1$, $N \leftrightarrow 2$, $S \leftrightarrow 3$. Dále sestavme tzv. matici přechodu[35] $\mathbb{P} \in \mathbb{R}^{3,3}$ jejíž prvek $\mathbb{P}_{ij}$ udává pravděpodobnost

[33] Andrey Andreyevich Markov, ruský matematik, 1856–1922.

[34] Příklad je převzat z monografie *Introduction to Probability Models* od S.M. Rosse. Na markovské řetězce lze narazit i v řadě skutečně praktických úloh.

[35] Neplést s maticí přechodu ve smyslu přechodu mezi bázemi, zde je o přechod mezi jednotlivými kroky řetězce.

přechodu ze stavu j do stavu i, kde $i, j \in \hat{3}$. V našem případě tedy platí[36]

$$\mathbb{P} = \begin{pmatrix} 0.5 & 0.3 & 0.2 \\ 0.4 & 0.4 & 0.3 \\ 0.1 & 0.3 & 0.5 \end{pmatrix}.$$

Máme-li vektor $v = (v_1, v_2, v_3)^T$ udávající pravděpodobnosti, že se Pepa jeden den nachází v uvedených stavech, pak vektor $\mathbb{P} \cdot v$ udává pravděpodobnosti, že se v těchto stavech nachází druhý den.

Naším cílem je nalézt tzv. stacionární rozdělení pravděpodobností splňující

$$\mathbb{P} \cdot v = v,$$

tedy **vlastní vektor** matice $\mathbb{P}$ příslušející **vlastnímu číslu** 1, a navíc splňující

$$v_1 + v_2 + v_3 = 1, \quad v_1, v_2, v_2 \geq 0.$$

Za jistých doplňujících předpokladů lze dokázat, že takovýto vektor existuje a popisuje pravděpodobnosti, že má Pepa v libovolný den příslušnou náladu. V našem konkrétním příkladě přímočarým výpočtem zjistíme, že tímto vektorem je vektor

$$v = (0.33871, 0.370968, 0.290323)^T.$$

Pepa je proto nejpravděpodobněji v neutrální náladě. Nejméně pravděpodobné je, že ho nalezneme smutnícího.

Principal component analysis (PCA)

V této podkapitole si velmi stručně a pouze na intuitivní úrovni[37] ukážeme jednu z technik využívaných (mimo jiné) v analýze dat.

Mějme dánu sadu dat $X_j \in \mathbb{R}^k$, $j \in \hat{n}$. Vektor X_j je nyní vhodné si představovat jako bod k-rozměrném prostoru $\mathbb{R}^k$. Naším cílem je charakterizovat jakým způsobem jsou data v tomto prostoru rozložena a třeba této znalosti využít k snížení dimenzionality problému (body $\mathbb{R}^2$ se vizualizují lépe než v $\mathbb{R}^{100}$). Chtěli bychom rozložení dat co nejvěrněji popsat pomocí elipsoidu (v $\mathbb{R}^2$ si představte posunutou a rotovanou elipsu) a odhalit „v kterých směrech se data nejvíce mění“.

Za tímto účelem si spočteme průměrnou hodnotu (těžiště množiny $\{X_j\}_{j=1}^n$)

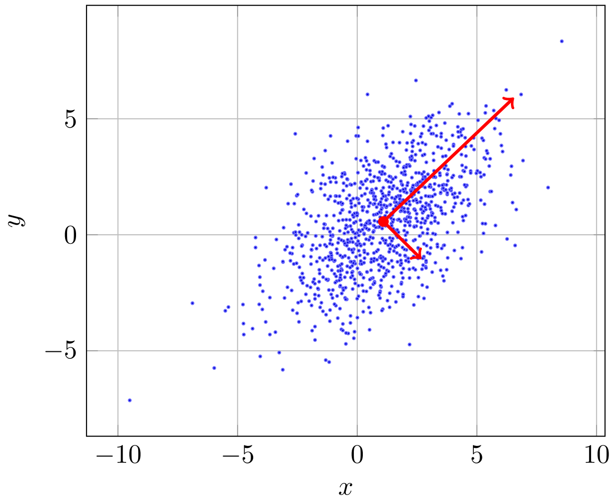
$$\bar{X} := \frac{1}{n} \sum_{j=1}^{n} X_j \in \mathbb{R}^k.$$

Dále sestavíme **kovarianční matici** $\mathbb{A} \in \mathbb{R}^{k,k}$ jejíž prvky splňují

$$\mathbb{A}_{i\ell} = \frac{1}{n} \sum_{j=1}^{n} \Big(X_{j,i} - \bar{X}_i\Big)\Big(X_{j,\ell} - \bar{X}_\ell\Big).$$

[36] Matice $\mathbb{P}$ je tzv. stochastická: její prvky jsou nezáporná čísla a součet v každém sloupečku je roven 1.

[37] To znamená, že některé části výkladu by šlo lépe popsat pomocí pojmů z teorie pravděpodobnosti a statistiky, což je nad rámec tohoto textu a tak může následující výklad působit místy vágně, protože vágní je.



Obrázek 7.2: Sada dat (modré body) a „hlavní komponenty" (červené šipky).

Tato reálná matice je tzv. symetrická, tj. platí pro ni vztah $\mathbb{A}^T = \mathbb{A}$. Lze ukázat, že každá symetrická matice je vždy diagonalizovatelná, její vlastní hodnoty jsou vždy reálné a vlastní vektory lze volit vzájemně kolmé.

Označme si vlastní čísla $\lambda_\ell \in \mathbb{R}$, $\ell \in k$, matice $\mathbb{A}$ v nerostoucím pořadí

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k.$$

Příslušné vlastní vektory nechť jsou označeny $u_1, u_2, \ldots, u_k \in \mathbb{R}^k$. Bez újmy na obecnosti můžeme předpokládat[38], že vlastní vektory jsou tzv. normalizovány na jedničku, tj. mají délku rovnou 1.

Pojďme si uvedený postup demonstrovat na jednoduchém příkladě graficky znázorněném na Obrázku č. 7.2. Data tvoří množina 1000 bodů v $\mathbb{R}^2$. Kovarianční matice je v tomto případě rovna

$$\mathbb{A} = \begin{pmatrix} 5.00224 & 2.6829 \\ 2.6829 & 4.88891 \end{pmatrix} \in \mathbb{R}^{2,2}$$

a průměr je $\bar{X} = (1.09435, 0.570682)^T$. Příslušná vlastní čísla seřazená podle velikosti jsou

$$\lambda_1 = 7.62908 \quad \text{a} \quad \lambda_2 = 2.26207,$$

a odpovídající vlastní vektory

$$u_1 = (5.45123, 5.33731)^T \quad \text{a} \quad u_2 = (1.58255, -1.61633)^T.$$

Vlastní vektory jsme naškálovali tak, aby měly délku rovnu právě příslušnému vlastnímu číslu.

Vlastní vektory uvedené v předchozím odstavci jsou znázorněny jako červené šipky na Obrázku č. 7.2. Vidíme, jak vektor odpovídající největšímu vlastnímu číslu nejlépe vystihuje dominantní směr, v kterém se data mění.

[38] Nenulový násobek vlastního vektoru je stále vlastní vektor příslušející stejnému vlastnímu číslu.

7.6 Dodatek: kam dál?

Na závěr uvedeme pouze několik poznámek doplňující výklad v této kapitole.

Poznámka 7.41 (Jordanův kanonický tvar)**.** *V podkapitole o diagonalizaci (Kapitola č. 7.4) jsme si ukázali matice, které nelze diagonalizovat. Přirozeně se nabízí otázka, jestli i tyto matice nelze převést podobnostní transformací do nějakého „kanonického" tvaru, z kterého bychom mohli vyčíst vlastní čísla i s jejich násobnostmi.*

Odpověď na tuto otázku je kladná. Každá matice $\mathbb{A} \in \mathbb{C}^{n,n}$ je podobná matici $\mathbb{J}$ v tzv. Jordanově kanonickém tvaru. Tato matice $\mathbb{J}$ je blokově diagonální. Jordanovy bloky mají tvar

$$\begin{pmatrix} \lambda & 1 & & & & & \\ 0 & \lambda & 1 & & & & \\ & 0 & \lambda & 1 & & & \\ & & \ddots & \ddots & \ddots & & \\ & & & 0 & \lambda & 1 & \\ & & & & 0 & \lambda & 1 \end{pmatrix}.$$

Připouští se i 1×1. Na diagonále matice $\mathbb{J}$ se vyskytují vlastní čísla matice $\mathbb{A}$ přesně tolikrát kolik je jejich algebraická násobnost.

Konstrukce příslušné podobnostní transformace je komplikovanější a její rozbor by byl nad rámec tohoto textu.

Poznámka 7.42 (*Singular value decomposition* (SVD))**.** *Proces diagonalizace matice lze zobecnit i na matice, které nejsou čtvercové. Máme-li matici $\mathbb{A} \in \mathbb{C}^{m,n}$, pak existují unitární*[39] *matice $\mathbb{U} \in \mathbb{C}^{m,m}$, $\mathbb{V} \in \mathbb{C}^{n,n}$ a diagonální*[40] *matice $\mathbb{S} \in \mathbb{C}^{m,n}$ splňující*[41]

$$\mathbb{A} = \mathbb{U} \cdot \mathbb{S} \cdot \overline{\mathbb{V}^T}.$$

Na tomto místě pouze zmíníme, že tento rozklad nachází široké uplatnění v mnoha zajímavých oblastech (k IT mají nejblíže asi různé metody zpracování signálu a statistika).

[39] Unitární matice je regulární matice jejíž sloupce jsou na sebe vzájemně kolmé a jsou normalizované na jedničku (vzhledem ke standardnímu skalárnímu součinu na $\mathbb{C}^n$).

[40] Pouze prvky $\mathbb{S}_{jj}$ mohou být nenulové.

[41] Pruh nad maticí označuje komplexní sdružení všech prvků příslušné matice.