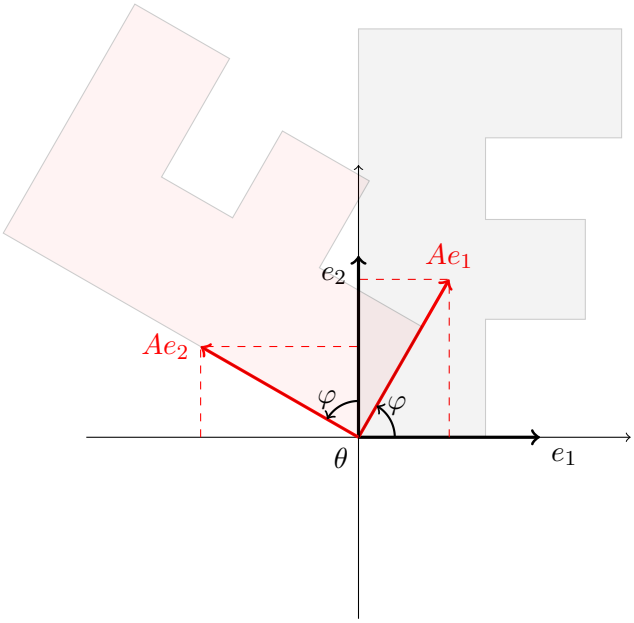
Lineární algebra

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 2019/2020

[1] Převážně kapitoly 2, 3 a 5.
[2] Převážně kapitoly 6 a 7.
[3] Převážně kapitoly 4 a 8, všeobecné zlepšování a korektury.
[4] Převážně kapitoly 1 a 4.

Obsah

Obsah ii

1 Soustavy lineárních rovnic 2
- 1.1 Co si z této kapitoly odneseme ... 3
- 1.2 Staré známé soustavy lineárních rovnic ... 4
- 1.3 Geometrická interpretace množiny řešení ... 6
- 1.4 Definice soustavy lineárních rovnic a snadno řešitelný případ ... 9
- 1.5 Matice a základní operace s nimi ... 13
- 1.6 Gaussova eliminační metoda (GEM) ... 23
- 1.7 Těleso ... 34

2 Základní pojmy lineární algebry 43
- 2.1 Co si z této kapitoly odneseme ... 44
- 2.2 Prostor šipek v rovině ... 44
- 2.3 Vektorový prostor ... 46
- 2.4 Lineární (ne)závislost ... 57
- 2.5 Lineární obal ... 62
- 2.6 Báze a dimenze ... 67

3 Hodnost matice a Frobeniova věta 85
- 3.1 Co si z této kapitoly odneseme ... 85
- 3.2 Hodnost matice ... 86
- 3.3 Regulární matice a maticová inverze ... 92
- 3.4 Frobeniova věta a kompletní řešení SLR ... 99
- 3.5 Lineární variety ... 109
- 3.6 Dodatky ... 117

4 Lineární kódy 120
- 4.1 Co si z této kapitoly odneseme ... 121
- 4.2 Základní pojmy a obecné vlastnosti samoopravných kódů ... 121
- 4.3 Lineární kódy ... 132
- 4.4 Dekódování ... 140

4.5 Dodatky 145

5 Lineární zobrazení **155**
5.1 Co si z této kapitoly odneseme 156
5.2 Základní pojmy 156
5.3 Linearita a její důsledky 157
5.4 Hodnost, jádro a defekt zobrazení 165
5.5 Matice lineárního zobrazení 172
5.6 Změna báze 183
5.7 Příklady lineárních zobrazení 187

6 Determinant matice **201**
6.1 Co si z této kapitoly odneseme 201
6.2 Motivace 201
6.3 Permutace 204
6.4 Definice determinantu matice 209
6.5 Vlastnosti determinantu matice 213
6.6 Výpočet determinantu matice 219
6.7 Shrnutí vlastností determinantu 223
6.8 Dodatky 224

7 Vlastní čísla a vlastní vektory **228**
7.1 Co si z této kapitoly odneseme 228
7.2 Motivace 229
7.3 Vlastní čísla a vlastní vektory lineárního operátoru 230
7.4 Diagonalizace lineárního operátoru a matice 247
7.5 Příklady 254
7.6 Dodatek: kam dál? 259

8 Skalární součin a ortogonalita **262**
8.1 Co si z této kapitoly odneseme 262
8.2 Skalární součin 263
8.3 Ortogonalita 267
8.4 Ortogonalita a symetrické matice 272

9 Přehled použitého značení **277**

Rejstřík **281**

Úvod

Milé studentky, milí studenti,

od akademického roku 2014/2015 se významně změnil kurz lineární algebry. Jednou z hlavních změn je, že namísto podrobných slajdů a handoutů je hlavním studijním materiálem tento studijní text. Tento text se snažíme neustále vylepšovat a doplňovat, může se tedy v průběhu semestru ještě měnit. 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 stránce kurzu BI-LIN na Course Pages.

Mnoho pěkných chvil při studiu lineární algebry přeje

Karel Klouda a kolektiv

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].

[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.

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 (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.

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

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 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:

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

[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.

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:

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

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

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 $\mathbb{R} \times \mathbb{R}$).

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

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:

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

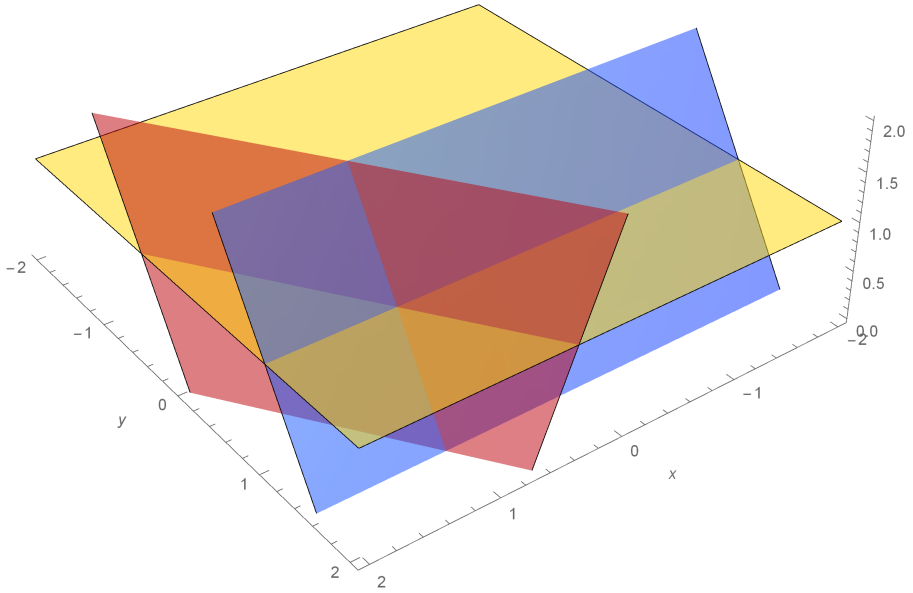
Jelikož jsou obě levé strany rovnic stejné, nemohou se pro žádnou trojici $(x, y, z) \in \mathbb{R}^3$ rovnat současně 3 i 4, a proto žádné řešení této soustavy neexistuje.

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

[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.

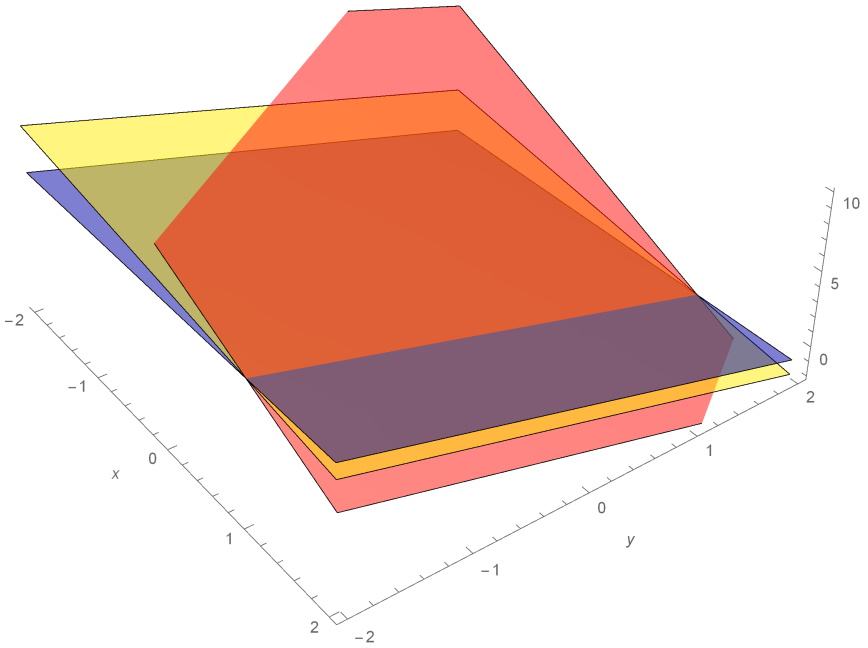
rovnici jedné neznámé $2y = 2$ a ta má jediné řešení $y = 1$. Podobně zjistíme, že první rovnice nám po dosazení za y a z říká, že $x = 1$.

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



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

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

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

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 $i \in \{1,\dots,m\}$ a $j \in \{1,\dots,n\}$ 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] $x_1,\dots,x_n \in \mathbb{R}$. Číslu a_{ij} říkáme **$j$tý koeficient $i$té rovnice**.*

*Množinu všech uspořádaných $n$tic $(x_1,x_2,\dots,x_n) \in \mathbb{R}^n$, 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 $(0, 0, \ldots, 0) \in \mathbb{R}^n$.*

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

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

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

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

kde S je množina řešení homogenní soustavy.

(vii) *Má-li homogenní soustava i jiné řešení než $(0, 0, \ldots, 0) \in \mathbb{R}^n$, 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 $(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$ platí

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

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

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

a tedy i $(\alpha x_1, \alpha x_2, \ldots, \alpha x_n) \in \mathbb{R}^n$ 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

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

[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** $\to$ **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!

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 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 každou soustavu 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:

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

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

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

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 $1 \leq i \leq m$, je stejná jako množina řešení rovnice

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

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

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

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

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.

[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.

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 $\mathbb{A}^3 = \mathbb{A} \cdot \mathbb{A} \cdot \mathbb{A}$).

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:*

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

[16] Do dvourozměrného pole, chcete-li.

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 matic definováno po složkách a sčítání reálných čísel je komutativní, je i sčítání matic komutativní. Platí tedy*

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

3. *Jelikož je sčítání matic a násobení matice číslem definováno po složkách, plyne z toho, že sčítání a násobení reálných čísel splňuje distributivní zákon, to, že 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 $\mathbb{D} = \mathbb{A}\mathbb{B}$.

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

[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.

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 $1 \leq i \leq m$ a $1 \leq j \leq t$:

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

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

[19] Samozřejmě.

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].

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 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

[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.

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 $m$prvkové **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.*

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 $\mathbb{A}\mathbb{x} = \mathbb{b}$.*

[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.

[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 $\mathbb{R}^{m,n+1}$.

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* $\mathbb{y} = \mathbb{x} + \mathbb{z}$.

(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 $\mathbb{b} + \theta = \mathbb{b}$:

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

□

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

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.

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.

[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.

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 schopni:

- 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 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 říkaly, se postaráme v další kapitole.

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

[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.

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:

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

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* $i \in \{1, 2, \ldots, n\}$ *(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 schopni 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

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

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

[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 současně první a třetí bod se říká **horní trojúhelníkové**.

[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 $\pi = 0$.

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 řešení je více? Ano, koukněme třeba na následující soustavu tří rovnic o pěti neznámých $(x_1, x_2, x_3, x_4, x_5)$:

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

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)

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

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

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

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 až

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

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

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

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

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. *Často 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. *Pro přehlednější zápis si zavedeme následující značení: Je-li* $n \in \mathbb{N}$ *potom definujeme*

$$\hat{n} = \{1, 2, \ldots, n\}.$$

[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.

Definice 1.26 (HST). *O matici $\mathbb{D} \in \mathbb{R}^{m,n}$ řekneme, že je v **horním stupňovitém tvaru**, jestliže všechny řádky jsou nulové, nebo existuje $k \in \hat{m}$ tak, že řádky 1 až k matice $\mathbb{D}$ jsou nenulové a řádky $k+1$ až m jsou nulové*[34] *a jestliže platí následující:*

Označme pro každé $i \in \hat{k}$ index nejlevějšího nenulového prvku v $i$tém řádku jako j_i, tj.

$$j_i = \min\{\ell \in \hat{n} \mid \mathbb{D}_{i\ell} \neq 0\}.$$

Potom platí $1 \leq j_1 < j_2 < \cdots < j_k$.[35]

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

O soustavě $\mathbb{A}\mathbb{x} = \mathbb{b}$ řekneme, že je v horním stupňovitém tvaru, pokud matice této soustavy $(\mathbb{A} \mid \mathbb{b})$ je v horním stupňovitém tvaru.

Poznámka 1.27. *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 snadnější představu přikládáme schéma obecné matice $\mathbb{D}$ v horním stupňovitém tvaru:

$$\begin{pmatrix}
0 & \cdots & 0 & \underbrace{\mathbb{D}_{1j_1}}_{\neq 0} & \cdots & * & * & \cdots & * & * & \cdots & * & * & \cdots & * \\
0 & \cdots & 0 & 0 & \cdots & 0 & \underbrace{\mathbb{D}_{2j_2}}_{\neq 0} & \cdots & * & * & \cdots & * & * & \cdots & * \\
0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & \underbrace{\mathbb{D}_{3j_3}}_{\neq 0} & \cdots & * & * & \cdots & * \\
\vdots & & & \vdots & & & \vdots & & & \vdots & \ddots & & \vdots & & \vdots \\
0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & \underbrace{\mathbb{D}_{kj_k}}_{\neq 0} & \cdots & * \\
0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\
\vdots & & & \vdots & & & \vdots & & & \vdots & & & \vdots & & \vdots \\
0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0
\end{pmatrix}$$

Pro ujasnění značení uveďme následující příklad (používá značení z Definice 1.26):

Příklad 1.28. *Pro soustavu (1.11) platí*

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

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

[35] Neboli první nenulové číslo nenulového řádku je vždy napravo od prvního nenulového prvku o řádek výše.

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 1.29. *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 $\left(0 \quad 0 \quad \cdots \quad 0 \mid c\right)$, kde c je nenulové číslo. To ale odpovídá rovnici $0 = c$, která nemá řešení. Řešení tedy nemá ani soustava rovnic[36].

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.

[36] Vzpomeňme tvrzení *(ii)* v Pozorování 1.4.

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 $\mathbb{A}$ (nikoliv $(\mathbb{A} \mid \mathbb{b})$) položíme rovny nule. Je jasné, že tyto proměnné nebudou mít poté žádný vliv na ostatní proměnné, proto můžeme jejich odpovídající sloupce ignorovat. 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[37] 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[38] tyto operace:

(G1) Prohození dvou řádků.

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

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

[37] 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.

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

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 1.30. *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 s nenulovým prvním sloupcem umíme převést pomocí (G1) až (G3) do tvaru, kdy má v prvním sloupci nenulový prvek pouze v prvním řádku[39]. 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 1.31. *Nechť $a, b \in \mathbb{R}$. Potom $x = -a + b$ je jediné reálné číslo splňující rovnici $a + x = b$.*

[39] Čistě nulový sloupec nám při řešení pochopitelně nevadí, znamená, že řešení zadané soustavy na jedné z proměnných vůbec nezáleží a lze ji volit libovolně.

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 (GEM)**:

Algoritmus 1.32 (GEM)**.** *Cíl algoritmu: Pro matici $\mathbb{B} \in \mathbb{R}^{m,n}$, hledáme takovou posloupnost úprav (G1) a (G3), která ji převede do horního stupňovitého tvaru. Postup: Položme $\mathbb{B} = (\mathbb{A} \mid \mathbb{b})$, $k = \ell = 1$. Dokud je $k \leq n$ a $\ell \leq m$, provádíme následující:*

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

2. *Je-li $\mathbb{B}_{\ell k} = 0$ a $\mathbb{B}_{jk} \neq 0$ pro nějaké $j \in \{\ell + 1, m\}$ prohodíme pomocí pravidla (G1) $j$tý a ℓtý řádek a pokračujeme do kroku 3.*

3. *Máme $\mathbb{B}_{\ell k} \neq 0$. Pomocí (G3) odečteme od všech spodnějších řádků vhodný násobek ℓtého řádku tak, abychom vynuluvali všechny prvky ktého sloupce pod prvkem na ℓtém řádku. Položte $k = k + 1$, $\ell = \ell + 1$ a pokračujme krokem 1.*

Pokud Vám tento popis není blízký[40], můžeme si algoritmus převyprávět:

- V prvním kroku zleva doprava vynecháváme sloupce, dokud nenarazíme na nenulový sloupec.
- V druhém kroku vhodně prohodíme řádky (G1) tak, aby první řádek měl na začátku nenulové číslo.
- V třetím kroku vytvoříme pomocí odečítání vhodného násobku prvního řádku (G3) schod v prvním sloupci (tj. nulové prvky na začátku 2. až posledního řádku). Vynecháme první řádek a první sloupec matice a pokračujeme krokem 1, dokud jsme nevynechali všechny řádky nebo sloupce.

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 můžeme významně ulehčit.

Uveďme si pro ilustraci běhu GEM následující příklad.

Příklad 1.33. *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 1.32 odpovídají následující úpravy:

$$\left(\begin{array}{ccccc|c} 6 & 0 & 0 & 1 & 1 & 6 \\ 2 & 8 & 1 & 0 & 0 & -5 \\ 3 & 6 & 3 & 9 & 0 & -9 \end{array}\right) \xrightarrow[\check{r}1 \leftrightarrow \check{r}3]{G1} \left(\begin{array}{ccccc|c} 3 & 6 & 3 & 9 & 0 & -9 \\ 2 & 8 & 1 & 0 & 0 & -5 \\ 6 & 0 & 0 & 1 & 1 & 6 \end{array}\right) \xrightarrow[1/3*\check{r}1]{G2}$$

$$\left(\begin{array}{ccccc|c} 1 & 2 & 1 & 3 & 0 & -3 \\ 2 & 8 & 1 & 0 & 0 & -5 \\ 6 & 0 & 0 & 1 & 1 & 6 \end{array}\right) \xrightarrow[\check{r}2-2*\check{r}1]{G3} \left(\begin{array}{ccccc|c} 1 & 2 & 1 & 3 & 0 & -3 \\ 0 & 4 & -1 & -6 & 0 & 1 \\ 6 & 0 & 0 & 1 & 1 & 6 \end{array}\right) \xrightarrow[\check{r}3-6*\check{r}1]{G3}$$

$$\left(\begin{array}{ccccc|c} 1 & 2 & 1 & 3 & 0 & -3 \\ 0 & 4 & -1 & -6 & 0 & 1 \\ 0 & -12 & -6 & -17 & 1 & 24 \end{array}\right)$$

Nyní jsme se v Algoritmu 1.32 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,

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

musíme provést G3 a nulu si vyrobit: přičteme k třetímu řádku trojnásobek druhého (to zapisujeme jako $\xrightarrow[\check{r}3+3*\check{r}2]{G3}$*) 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 1.29 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 1.29. 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, které 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[41] 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 $3x = 1$).

[41] Po hříchu oblíbenější.

Příklad 1.34. *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 1.29 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[42] pro všechna α z $\mathbb{Q}$ resp. $\mathbb{R}$ resp. $\mathbb{C}$. Toto znamená, že např.

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

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 1.29 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 1.29, protože ta kvůli neexistenci (multiplikativních) inverzí[43] neplatí.

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

[43] A tedy i neplatnosti Věty 1.1.

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[44] $\{0, 1, \ldots, n-1\}$. 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[45]. 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

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

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 1.35. *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

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

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

$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. 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 1.36. *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[46].

Lemma 1.37. *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[47]. 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!

[46] 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.

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

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 1.31. Ještě jednou si ji dokážeme[48]. 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 1.38. *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) $\forall a \in M, \exists a^{-1} \in M : a \circ a^{-1} = a^{-1} \circ a = e$ *(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 1.39. *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 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 1.40. *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.

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

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

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

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 1.31 zahodit, neboť jsou okamžitým důsledkem předchozí věty a faktu, že $(\mathbb{R}, +)$ a $(\mathbb{R} \setminus \{0\}, \cdot)$ jsou grupy[49].

Věta 1.40 platí pro jakoukoli grupu, tedy i pro ty, se kterými jsme se doposud setkali. Pro přehlednost je shrňme v následujícím pozorování.

Pozorování 1.41. *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:

Definice 1.42. *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* ***nulovým prvkem****),*

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

(iii) platí levý a pravý[50] *distributivní zákon, tj.*

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

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

[50] 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.

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

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

Poznámka 1.43. *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 $0 = u - u = (u + u) - u = u + (u - u) = u + 0 = u$.[51]

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

Věta 1.44. *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 1.45. *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, operace sčítání, násobení, transpozice s těmito maticemi, 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[52], příp. nemá řešení žádné.

Dodatek ke konečným tělesům

Konečná tělesa jsou pro informatiky primárně důležitá tím, že se v nich kóduje a šifruje. O kódování budeme mluvit později v Kapitole 4, o šifrování se více dozvíte v kurzu BI-BEZ[53].

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

[51] 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 $0a = 0$.

[52] 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.

[53] Bezpečnost, letní semestr druhého ročníku.

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). Obvyklé značení takovéhoto tělesa je $GF(p^k)$.[54] Tělesa s počtem prvků p jsme si ukázali, jsou to právě tělesa $\mathbb{Z}_p$, tedy $\mathbb{Z}_p = GF(p^1)$.

Konstrukce těchto těles není obtížná, jen je nad rámec našeho základního kurzu lineární algebry. Zájemcům můžeme doporučit nakouknout do materiálů MI-MPI[55], jak se tato tělesa s neprvočíselným počtem prvků konstruují, a také doporučit MI-MKY[56], kde uvidí jejich aplikaci.

[54] GF = Galois field, neboli Galoisovo těleso.

[55] Matematika pro informatiku, zimní semestr prvního ročníku magisterského studia.

[56] Matematika pro kryptologii, letní semestr prvního ročníku magisterského studia.

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).

[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…

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.

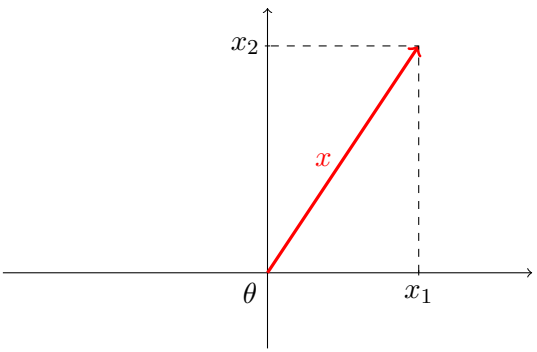
3. Smíříme se s tím, že postup „od obecného ke konkrétnímu“ je mnohem výhodnější, než ten opačný[5]. Namísto dokazování různých pravd a vlastností v každém konkrétním vektorovém prostoru zvlášť je totiž stačí dokázat jen jednou – pro libovolný vektorový prostor, pouze s využitím axiomů a z nich odvozených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

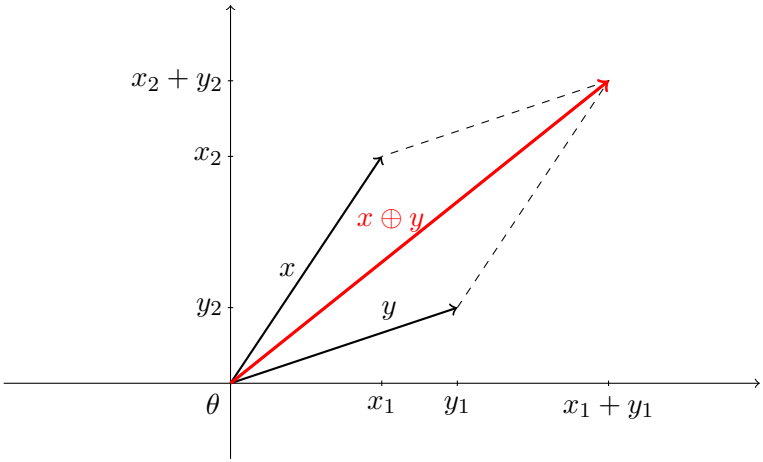


[5] Nebo se o to budeme alespoň usilovně snažit. Typický student je často navyklý obrácenému postupu a tvrdohlavě začíná pitváním se v příliš konkrétních příkladech – z těch se pak pokouší vyvozovat obecná tvrzení. To sice může pomoci v těžkých začátcích a i my v textu obvykle začínáme příklady, nicméně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

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

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

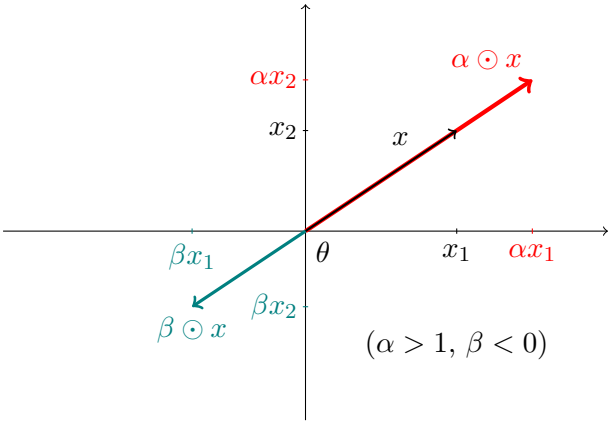
pak odpovídá přirozenému skládání orientovaných úseček:



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]),

[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.

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):*

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

[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 $\mathbb{R}^2$.

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, pěticemi,... 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 „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 1.42) 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. $\forall a \in V : 1 \odot a = a$,

[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 $n = 4$.

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

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

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 zdát 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,*

[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.

[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.

1. *Nejprve zvolíme vhodné číselné těleso – jeho axiomy nám vlastně zaručují, že se skaláry „půjde rozumně pracovat“, viz Definice 1.42.*

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!

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.,*

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

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

(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

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

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

$$a \overset{(A6)}{=} 1 \cdot a = (\alpha^{-1}\alpha)a \overset{(A3)}{=} \alpha^{-1} \cdot (\alpha a) = \alpha^{-1} \cdot \theta \overset{(2)}{=} \theta. \qquad \square$$

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.

[16] A nadmíru ochotně.

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

$$x + y = (x_1, \dots, x_n) + (y_1, \dots, y_n) := (x_1 + y_1, \dots, x_n + y_n)\,,$$
$$\alpha x = \alpha(x_1, \dots, x_n) := (\alpha x_1, \dots, \alpha x_n)\,,$$

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

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

je vektorový prostor.

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

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

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].

[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.

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 $a \in \mathbb{R}^1$ 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].

[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.

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

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 $\emptyset \neq P \subseteq V$ (P je neprázdná podmnožina V). Říkáme, že P je **podprostor** prostoru V, právě když platí:*

1. $\forall x, y \in P$: $x + y \in P$,
2. $\forall \alpha \in T, \forall x \in P$: $\alpha x \in P$

*(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.

[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 $P \times P \subseteq V \times V$.

- 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]. □

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.

[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.

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

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

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

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

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 pojmem* 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

(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 $\alpha x \in P \cap Q$:

[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 $\alpha \in T$!

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

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

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

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

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 podprostorů 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

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

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**!

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

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

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

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

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

Definice 2.24. *Nechť $(x_1, \ldots, x_n)$ je soubor vektorů z V. Řekneme, že $(x_1, \ldots, x_n)$ 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]*:*

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

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

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

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

[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!

[30] Jazykem predikátové logiky.

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 délky alespoň dva vznikne LN soubor.

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

(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

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

[31] Tedy dokázat…

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

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 $(x_1, \ldots, x_n)$ ve VP V ověřte, zda je LN nebo LZ.*

1. *Hledáme, jestli existuje i jiná ntice koeficientů $\alpha_1, \ldots, \alpha_n \in T$ než $(0, \ldots, 0)$ taková, že příslušná lineární kombinace je rovna nulovému vektoru.*
2. *Koeficienty $\alpha_1, \ldots, \alpha_n \in T$ považujme za neznámé v rovnici*
$$\alpha_1 x_1 + \cdots + \alpha_n x_n = \theta.$$
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 1.29 určeme, kolik existuje řešení.*
5. *Existuje-li jediné řešení $(\alpha_1, \ldots, \alpha_n) = (0, \ldots, 0)$, je zadaný soubor LN, v opačném případě je LZ.*

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

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

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*

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

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

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

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 $(\alpha,\beta,\gamma,\delta) \in \{(0,0,0,0),(1$
Zadaný soubor je tedy LZ.

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

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, $\emptyset \neq M \subseteq V$. 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*

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

Buď $\emptyset \neq M \subseteq V$. 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 neprázdná podmnožina vektorového prostoru V. Pak platí:*

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

[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.

(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). Tedy existují soubory $(x_1, \ldots, x_k)$ a $(y_1, \ldots, y_\ell)$ vektorů z M a koeficienty $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_\ell \in T$ takové, že platí

$$\left(x = \sum_{i=1}^{k} \alpha_i x_i\right) \wedge \left(y = \sum_{i=1}^{\ell} \beta_i y_i\right) \Rightarrow (x + y) = \alpha_1 x_1 + \cdots + \alpha_k x_k + \beta_1 y_1 + \cdots + \beta_\ell y_\ell \,.$$

Zřejmě platí, že $(k+\ell)$-tice $(x_1, \ldots, x_k, y_1, \ldots, y_\ell)$ je také soubor vektorů z M[38] a tedy $x + y \in \langle M \rangle$. 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.*
- *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

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

[38] Rozmyslete si například, že případné duplicity $x_i = y_j$ nijak neodporují definici souboru.

- *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[39] v bodě (v) Pozorování 2.32

(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 $M \subseteq \langle M \rangle$. 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 $x \in M$. □

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

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![40]

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

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

Důkaz. Dokážeme dvě implikace:

1. $(\Rightarrow)$: Je-li soubor $(x_1, \ldots, x_n)$ LZ, existují $\alpha_1, \ldots, \alpha_n \in T$ 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[41] α_k) na[42]

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

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

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. □

[40] A to se vědět vyplatí!

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

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

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“[43] 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[44] 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.

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 $\mathbb{B}$.*

Speciálně pro libovolné $\mathfrak{a} = (a_1\ a_2\ \cdots\ a_n) \in T^{1,n}, \mathfrak{b} = (b_1\ b_2\ \cdots\ b_n)^T \in T^{n,1}$ platí vztahy

$$\mathfrak{a} \cdot \mathbb{B} = \sum_{i=1}^{n} a_i \mathbb{B}_{i:} , \qquad \mathbb{A} \cdot \mathfrak{b} = \sum_{j=1}^{n} b_j \mathbb{A}_{:j} .$$

[43] Což je jen vágní a nijak nedefinovaný pojem.

[44] Opět si láskyplně vzpomeneme na axiomy tělesa…

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

$$(\mathbb{AB})_{ij} = \sum_{\ell=1}^{n} \mathbb{A}_{i\ell}\mathbb{B}_{\ell j} = \sum_{\ell=1}^{n} \mathbb{B}_{\ell j}\mathbb{A}_{i\ell}$$

a proto pro každé $j \in \hat{k}$ je

$$(\mathbb{AB})_{:j} = \begin{pmatrix} (\mathbb{AB})_{1j} \\ (\mathbb{AB})_{2j} \\ \vdots \\ (\mathbb{AB})_{mj} \end{pmatrix} = \begin{pmatrix} \sum_{\ell=1}^{n} \mathbb{B}_{\ell j}\mathbb{A}_{1\ell} \\ \sum_{\ell=1}^{n} \mathbb{B}_{\ell j}\mathbb{A}_{2\ell} \\ \vdots \\ \sum_{\ell=1}^{n} \mathbb{B}_{\ell j}\mathbb{A}_{m\ell} \end{pmatrix} = \sum_{\ell=1}^{n} \mathbb{B}_{\ell j} \begin{pmatrix} \mathbb{A}_{1\ell} \\ \mathbb{A}_{2\ell} \\ \vdots \\ \mathbb{A}_{m\ell} \end{pmatrix} = \sum_{\ell=1}^{n} \mathbb{B}_{\ell j}\mathbb{A}_{:\ell}.$$

Tedy $j$tý sloupec matice $\mathbb{AB}$ je lineární kombinací sloupců matice $\mathbb{A}$.

Závěr tvrzení pak jakožto speciální případ plyne z již dokázaného (s volbou jednořádkové matice $\mathbb{A}$ či jednosloupcové matice $\mathbb{B}$). □

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[45] 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“[46] 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“[47]. 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.

[45] Jeden z nekonečně mnoha.

[46] Velmi lidově řečeno...

[47] Vzpomeňme na Důsledek 2.37 o lineárně závislých souborech vektorů.

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*

(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 $\alpha_1, \ldots, \alpha$ 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 1.29 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.[48]

Postup ilustrujeme na příkladech souborů z Příkladů 2.28 a 2.29, pouze místo lineární nezávislosti zkoumáme druhou vlastnost bází.

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*

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

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*

$$\alpha\begin{pmatrix}1&0\\1&1\end{pmatrix}+\beta\begin{pmatrix}0&2\\0&1\end{pmatrix}+\gamma\begin{pmatrix}1&0\\1&2\end{pmatrix}+\delta\begin{pmatrix}0&1\\0&0\end{pmatrix}=v=\begin{pmatrix}v_{11}&v_{12}\\v_{21}&v_{22}\end{pmatrix}.$$

[48] Přemýšlivý student jistě snadno dojde k podmínce, v jakém tvaru musí matice soustavy být, aby byl zkoumaný soubor bází – vzpomeňme na Pozorování 1.23.

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[49] *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.*

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*[50], *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*

$$\begin{aligned} e_1 &:= (1, 0, 0, 0, \dots), \\ e_2 &:= (0, 1, 0, 0, \dots), \\ e_3 &:= (0, 0, 1, 0, \dots), \\ &\vdots \end{aligned}$$

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

[50] I zde rozumíme $0, 1 \in T$.

tedy pro každé $k \in \mathbb{N}$ je e_k nekonečná posloupnost nul s jedinou jedničkou na kté 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. Řekneme, že dimenze vektorového prostoru V je rovna*

- $\mathbf{0}$*, pokud ve V neexistuje LN soubor délky* 1*.*
- $\mathbf{n} \in \mathbb{N}$*, pokud ve V existuje LN soubor délky n, ale každý soubor délky $n+1$ už je nutně LZ.*
- $\boldsymbol{\infty}$*, pokud ve V existuje LN soubor libovolné délky.*

Dimenzi vektorového prostoru V označujeme symbolem $\dim V$*.*

Je-li $\dim V = \infty$*, říkáme, že V **má nekonečnou dimenzi**, naopak pokud* $\dim V < \infty$ *říkáme, že V **má konečnou dimenzi**.*

Poznámka 2.47. *Na první pohled nemusí být jasné, že předchozí definice je korektně definovaný pojem. Proto si její korektnost ukažme. Nejdříve si všimněme, že z Pozorování 2.25 plyne*

$$\text{Existuje-li LN soubor délky } n \in \mathbb{N} \implies \text{existuje LN soubor libovolné délky } i \in \hat{n}.$$

Dimenze V vždy existuje. Není-li dimenze nekonečná, ukážeme, že je konečná. Mějme $k \in \mathbb{N}$ nejmenší takové, že neexistuje žádný LN soubor délky $k \in \mathbb{N}$. Je-li $k = 1$ tak to přesně znamená, že $\dim V = 0$*. Pro $k \geq 2$ dostáváme z minimality k to, že existuje LN soubor délky $k-1$ a každý soubor délky k je LZ. Nebo-li* $\dim V = k - 1$*.*

Dimenze V je jednoznačná. Nemůže nastat případ takový, že by existovala čísla $m < n \in \{0, 1, \dots, \infty\}$ taková, že by obě splňovala podmínku pro dimenzi V. Z předchozího vztahu a toho, že $m < n$, by vyplynulo, že existuje LN soubor délky $m+1$ a $\dim V$ *by tedy nemohla být rovna m.*

Příklad 2.48. *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[51]) je lineárně závislý. Přímo z definice dostáváme*

$$\dim \mathbb{R}^2 = 2.$$

Podobně bychom v $\mathbb{R}^3$ zjistili, že $\dim \mathbb{R}^3 = 3$*.*

[51] Skutečně, zopakujte si, co platí pro každý LZ soubor, do kterého přidáme další vektor.

Vášnivý čtenář jiných textů o lineární algebře by zde mohl namítnout, že naše definice dimenze je, lidově řečeno, „nějaká podivná“ – že on[52] 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[53], 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 2.49.

(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* $n \in \mathbb{N}$ *a nechť je ve* V *každý* n*-členný soubor LZ. Potom*

$$\dim V \leq n - 1.$$

Důkaz. 1. Je-li $\dim V = 0$, potom z definice každý jednočlenný soubor vektorů ve V je LZ. Z Pozorování 2.25 nutně plyne, že každý takový soubor může obsahovat jen nulový vektor. Tedy ve V leží pouze θ, nebo-li $V = \{\theta\}$.

Je-li naopak $V = \{\theta\}$, pak jediný soubor délky 1 je (θ) a ten je LZ.

2. V triviálním vektorovém prostoru neexistuje žádný LN soubor, tudíž $\{\theta\}$ nemůže mít bázi.

3. Z definice dimenze plyne, že $\dim V \notin \{0, 1, 2 \ldots n-1\}$. Proto $\dim V \geq n$.

4. Opět z definice dimenze máme, že $\dim V \notin \{n, n+1 \ldots, \infty\}$. Proto $\dim V \leq n-1$. □

[52] Či ona!

[53] Můžete si vyhledat termín Occamova břitva, jde o myšlenkově blízký pojem.

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 některých důkazech potřebovat, je takzvané Steinitzovo lemma o výměně. Je poměrně technické, proto jeho důkaz nebudeme v kurzu BI-LIN vyžadovat.

Lemma 2.50 (Steinitzovo o výměně)**.** *Nechť $\mathcal{X} = (x_1, \ldots, x_n)$ a $\mathcal{Y} = (y_1, \ldots, y_m)$ jsou soubory vektorů z V. Předpokládejme, že je soubor $\mathcal{X}$ LN a současně $\forall i \in \hat{n} : x_i \in \langle \mathcal{Y} \rangle$.*[54] *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

$$\langle y_1, \ldots, y_m \rangle = \langle x_1, \ldots, x_n, (y_i \mid i \in \hat{m} \setminus \{i_1, i_2, \ldots, i_n\}) \rangle.$$[55]

Důkaz. Důkaz provedeme indukcí. Předpokládejme, že umíme vyměnit $k-1$ vektorů z $\mathcal{Y}$ těmi z $\mathcal{X}$, pro nějaké $k \in \{1, \ldots, n-1\}$. Zřejmě pro $k = 1$ to umíme triviálně. Ukážeme, jak vyměnit $k$tý vektor.

Na začátku $k$tého kroku máme

$$x_k \in \langle y_1, \ldots, y_m \rangle = \langle x_1, \ldots, x_{k-1}, (y_i \mid i \in \hat{m} \setminus \{i_1, i_2, \ldots, i_{k-1}\}) \rangle$$

V případě $k = 1$ jsme na pravé straně nenahradili ani jeden vektor z $\mathcal{Y}$.

Tedy

$$x_k = \sum_{i=1}^{k-1} \alpha_i x_i + \sum_{i \in \hat{m} \setminus \{i_1, i_2, \ldots, i_{k-1}\}} \beta_i y_i.$$

Ukažme si, že alespoň jeden ze koeficientů β_i musí být pro nějaké $i \in \hat{m} \setminus \{i_1, i_2, \ldots, i_{k-1}\}$ nenulový: Kdyby ne, tak platí v případě $k > 1$ to, že $x_k = \sum_{i=1}^{k-1} \alpha_i x_i$ neboli $x_k \in \langle x_1, \ldots, x_{k-1} \rangle$, což podle Věty 2.36 je spor s lineární nezávislostí souboru $\mathcal{X}$. Pro $k = 1$ obdržíme $x_k = \theta$, což opět díky lineární nezávislosti souboru $\mathcal{X}$ platit nemůže.

Poznamenejme, že jsme právě ukázali, že k musí být menší rovno m, z čehož vyplyne, že $n \leq m$.

---

[54] „Lidově“ řečeno $\mathcal{X}$ je generován souborem $\mathcal{Y}$.

[55] 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.

Označme si index tohoto nenulového koeficentu i_k, neboli $\beta_{i_k} \neq 0$. Potom

$$y_{i_k} = \sum_{i=1}^{k-1} -\beta_{i_k}^{-1}\alpha_i x_i \ + \ \beta_{i_k}^{-1} x_k \ + \sum_{i \in \hat{m} \setminus \{i_1, i_2, \ldots, i_k\}} -\beta_{i_k}^{-1}\beta_i y_i.$$

Konečně s pomocí Pozorování 2.32 (ii) obdržíme

$$\begin{aligned}\langle y_1, \ldots, y_m \rangle &= \langle x_1, \ldots, x_{k-1}, (y_i \mid i \in \hat{m} \setminus \{i_1, i_2, \ldots, i_{k-1}\}) \rangle \\ &= \langle x_1, \ldots, x_k, (y_i \mid i \in \hat{m} \setminus \{i_1, i_2, \ldots, i_{k-1}\}) \rangle \\ &= \langle x_1, \ldots, x_k, (y_i \mid i \in \hat{m} \setminus \{i_1, i_2, \ldots, i_k\}) \rangle\end{aligned}$$

□

Důsledek 2.51 (Důsledek Steinitzova lemmatu)**.** *Generuje-li soubor* $(y_1, \ldots, y_n)$ *vektorový prostor* V*, potom* $\dim V \leq n$.

Důkaz. Dle bodu (i) ze Steinitzova lemmatu 2.50 musí být každý soubor délky $n+1$ lineárně závislý. Proto dle Věty 2.49 je $\dim V \leq n$. □

Následující věta nám ušetří práci při hledání báze prostoru V konečné dimenze $n \in \mathbb{N}$. Jakmile ověříme jednu z vlastností *generuje V/je LN* souboru stejné délky n, obdržíme automaticky i druhou vlastnost.

Věta 2.52. *Nechť* $(x_1, \ldots, x_n)$ *je soubor vektorů z* V *a* $\dim V = n \in \mathbb{N}$*. Potom následující tvrzení jsou ekvivalentní:*

1. *Soubor* $(x_1, \ldots, x_n)$ *je báze* V*.*
2. *Soubor* $(x_1, \ldots, x_n)$ *je LN.*
3. *Soubor* $(x_1, \ldots, x_n)$ *generuje* V*.*

Důkaz. Implikace (1) $\implies$ (2) plyne přímo z definice báze.

Dokážeme (2) $\implies$ (3).

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 dle Věty 2.49, že $\dim V \geq n+1$, tedy spor.

Zbývá ukázat (3) $\implies$ (1).

Už víme, že soubor $(x_1, \ldots, x_n)$ generuje V, musíme dokázat, že je LN. Pro spor předpokládejme, že $(x_1, \ldots, x_n)$ je LZ. Je-li $n = 1$, tak to znamená, že $x_1 = \theta$ a $V = \langle \theta \rangle$, což je spor s $\dim V = 1$. Je-li $n \geq 2$ můžeme pomocí Důsledku 2.37 nalézt soubor délky $n-1$ generující V. Z Důsledku Steinitzova lemmatu 2.51 pak ale plyne, že $\dim V \leq n-1$, což je spor. □

Věta 2.53. *Nechť* $\dim V = n \in \mathbb{N}$. *Potom ve* V *existuje* n*-členná báze.*

Důkaz. Protože $\dim V = n$, existuje z definice dimenze LN soubor délky n. Z předchozí Věty 2.52 víme, že je to báze V. □

Věta 2.54. *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 n-člennou bázi V jako $(y_1, \ldots, y_n)$. Víme, že existence n-prvkového LN souboru implikuje $\dim V \geq n$. Na druhou stranu $(y_1, \ldots, y_n)$ generuje V a z Důsledku Steinitzova lemmatu 2.51 plyne $\dim V \leq n$. Proto je v tomto případě $\dim V = n$.

Existuje-li ve V nekonečná báze, pak ve V existují LN soubory libovolné délky (libovolné konečné podmnožiny této báze), proto je v takovém případě podle definice dimenze $\dim V = \infty$. □

Důsledek 2.55. *Všechny báze vektorového prostoru* V *mají stejný počet prvků, roven* $\dim V$.

Důkaz. Předpokládejme nejprve, že ve V existují dvě konečné báze, jedna s $m \in \mathbb{N} \cup \{\infty\}$ vektory a druhá s $n \in \mathbb{N} \cup \{\infty\}$ vektory. Podle předchozí věty potom $m = \dim V$ a současně $n = \dim V$. Dimenze V je ale jednoznačně určené číslo, a proto $m = n$. □

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 2.56. *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 je zopakování Důsledku Steinitzova lemmatu 2.51. 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 2.57. *Nechť $(x_1, \dots, x_k)$ je LN soubor vektorů z V a $\dim V = n \in \mathbb{N}$. Potom existují vektory $x_{k+1}, \dots, x_n \in V$ takové, že $(x_1, \dots, x_n)$ 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 n-členný soubor generátorů obsahující vektory $x_1, \dots, x_k$. Z Věty 2.52 plyne, že je to báze. □

Poznámka 2.58. *I když to v textu formálně nedokazujeme, důležitá tvrzení platí i pro prostory nekonečné dimenze pokud předpokládáme tzv. axiom výběru* [56]*:*

(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 2.59. *Z existence standardních bází (Příklad 2.45) lze rovnou vyvodit následující poznatky:*

- $\dim T^n = n$.
- $\dim T^{m,n} = mn$.

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[57]*.*

[56] Zájemce můžeme vřele odkázat na volitelný předmět letního semestru BI-ALO.

[57] Pozor, následující část vyzrazuje zápletku nebo rozuzlení díla: Bázi můžeme zvolit podobně jako standardní, například $\big((1, 0, \dots, 0), (i, 0, \dots, 0), \dots, (0, \dots, 0, 1), (0, \dots, 0, i)\big)$.

Příklad 2.60. *Rozmyslete si, že* $\mathcal{E}_\infty = (e_1, e_2, e_3, \dots)$, *kde*

$$\begin{aligned} e_1 &:= (1,0,0,0,\dots), \\ e_2 &:= (0,1,0,0,\dots), \\ e_3 &:= (0,0,1,0,\dots), \\ &\vdots \end{aligned}$$

netvoří *bázi* T^∞.[58]

Tyto vektory $\mathcal{E}_\infty$ *ale tvoří nekonečnou LN množinu a proto*

$$\dim T^\infty = \infty.$$

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 2.61. *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 $\dim P = \infty$, potom existuje v P a tedy i ve V LN soubor libovolné délky. Přímo z definice obdržíme, že $\dim P = \infty = \dim V$ a první tvrzení věty platí.

Nechť tedy $k := \dim P < \infty$ a $P \subset\subset V$. Je-li $k = 0$, tvrzení triviálně platí.[59] Máme-li $k \in \mathbb{N}$, potom z definice dimenze existuje LN soubor délky k vektorů z P. Tento soubor ale také leží ve V, proto z Věty 2.49 je $\dim V \geq k = \dim P$.

Zbývá nám dokázat druhou část věty. Buď nyní $P \subset\subset V$ vlastní podprostor, tj. $P \neq V$. Z předchozího kroku a předpokladu už víme, že

$$k := \dim P \leq \dim V < \infty,$$

chceme dokázat ostrou nerovnost $k < \dim V$.

Je-li $\dim P = 0$, tj. $P = \{\theta\}$, musí platit $V \neq \{\theta\}$, a tedy $\dim V \geq 1 > 0 = \dim P$ a nerovnost platí.

Je-li $\dim P = k \geq 1$, existuje k-členný LN soubor vektorů z P, označme jej $(x_1, \dots, x_k)$. Protože $P \neq V$, existuje $x_{k+1} \in V$ takový, že $x_{k+1} \notin P$. Potom soubor $(x_1, \dots, x_k, x_{k+1})$ je LN. Odkud rovnou plyne $\dim V \geq k+1 > k = \dim P$.

V obou případech platí $\dim P < \dim V$. □

[58] Dle definice lineárního obalu jsou povoleny pouze lineární kombinace konečně mnoha prvků!

[59] Zřejmě pro každé $n \in \mathbb{N}$, je $0 \leq n$ a samozřejmě platí $0 \leq \infty$.

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 2.62. *Buď $P \subset\subset V$ a $\dim P = \dim V < \infty$. Potom $P = V$.*

Poznámka 2.63. *Předpoklad $\dim V < \infty$ v druhé části tvrzení Věty 2.61 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 2.64. *Buď 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 $A \oplus B$[60].

Příklad 2.65. *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

$$E_1 \oplus E_2 = \mathbb{R}^2\,.$$[61]

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**.*

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 2.66. *Buďte $P \subset\subset V$, $Q \subset\subset V$. Potom $P + Q$ je direktní právě tehdy, když*

$$P \cap Q = \{\theta\}.$$

[60] Což si samozřejmě nebudeme plést s explicitně zdůrazněnou operací sčítání vektorů – jistě rozeznáme vektor od množiny.

[61] Nad tímhle se zkuste férově zamyslet.

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 $a_1 \neq a_2$ nebo $b_1 \neq b_2$. 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 $a_1 - a_2$ nebo $b_2 - b_1$, což je spor. □

Důležitou souvislost mezi dimenzemi podprostorů, jejich průniků a součtů dává 1. věta o dimenzi. Její důkaz si uvedeme pro úplnost textu a pro větší rozsah jej nebudeme vyžadovat.

Věta 2.67 (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:

$$\dim(P \oplus Q) = \dim P + \dim Q.$$

Důkaz. Je-li $P \subset\subset Q$ nebo $Q \subset\subset P$, vidíme, že tvrzení triviálně platí. Nechť tedy ani jeden podprostor není podprostorem druhého. Rozmysleme si, že je-li $\dim P = \infty$ nebo $\dim Q = \infty$, pak i $\dim P + Q = \infty$ a dokazovaný vztah platí.

Nechť tedy P i Q mají konečnou dimenzi. Začneme obtížnějším případem, kdy $P \cap Q \neq \{\theta\}$. Označme si $(x_1, \dots x_k)$ bázi $P \cap Q$.

Nalezneme vektory $y_1, \dots y_m, z_1, \dots z_n$ tak, aby $(x_1, \dots x_k, y_1, \dots y_m)$ byla báze P a $(x_1, \dots x_k, z_1, \dots z_n)$ byla báze Q. Ukážeme, že $(x_1, \dots x_k, y_1, \dots y_m, z_1, \dots z_n)$ je báze $P + Q$, čímž budeme hotovi, neboť

$$\dim(P + Q) + \dim(P \cap Q) = (k + m + n) + k = (k + m) + (k + n) = \dim P + \dim Q.$$

Z konstrukce je zřejmé, že tento soubor generuje $P+Q$. Zbývá dokázat jeho lineární nezávislost. Předpokládejme, že

$$\theta = \underbrace{\sum_{i=1}^{k} \alpha_i x_i}_{=:x} + \underbrace{\sum_{i=1}^{m} \beta_i y_i}_{=:y} + \underbrace{\sum_{i=1}^{n} \gamma_i z_i}_{=:z}. \tag{2.1}$$

Potom $z = -x - y$. Jelikož x i y patří do podprostoru P, patří tam i z. Vektor z patří ale i do Q. Tedy $z \in P \cap Q$. Díky tomu, že $(x_1, \dots x_k)$ je báze tohoto průniku, lze nalézt $\delta_1, \dots \delta_k$ tak, že

$$z = \sum_{i=1}^{k} \delta_i x_i.$$

Tedy

$$\theta = z - \sum_{j=1}^{k} \delta_j x_j = \sum_{i=1}^{n} \gamma_i z_i + \sum_{j=1}^{k} (-\delta_j) x_j.$$

Z lineární nezávislosti souboru $(x_1, \dots x_k, z_1, \dots z_n)$ plyne $\gamma_i = 0 = \delta_j$ pro $i \in \hat{n}$, $j \in \hat{k}$. Proto se rovnice (2.1) redukuje do tvaru

$$\theta = \sum_{i=1}^{k} \alpha_i x_i + \sum_{i=1}^{m} \beta_i y_i.$$

Ale soubor $(x_1, \dots x_k, y_1, \dots y_m)$ je lineárně nezávislý, proto i $\alpha_i = 0 = \beta_j$ pro $i \in \hat{k}$, $j \in \hat{m}$. Tedy všechny koeficienty v (2.1) musí být nulové a celý soubor $(x_1, \dots x_k, y_1, \dots y_m, z_1$ je lineárně nezávislý.

Případ $P \cap Q = \{\theta\}$ se dokáže analogicky. □

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[62].

Pozorování 2.68. *Buďte $(x_1, \dots, x_n)$ a $(y_1, \dots, y_m)$ dva soubory vektorů z V. Potom*

$$\langle x_1, \dots, x_n \rangle = \langle y_1, \dots, y_m \rangle$$

právě tehdy, když

$$\dim\langle x_1, \dots, x_n \rangle = \dim\langle y_1, \dots, y_m \rangle = \dim\langle x_1, \dots, x_n, y_1, \dots, y_m \rangle.$$

[62] 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!

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 2.62. 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 2.69. *Budeme-li chtít v následujícím textu explicitně zdůraznit, že uvažovaný vektorový prostor V má konečnou dimenzi $n \in \mathbb{N}$, a přitom šetřit místem, budeme jej značit V_n.*

Věta 2.70. *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[63] 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 2.71. *Nechť $\mathcal{X} = (x_1, \ldots, x_n)$ je báze V_n a vektor $z \in V_n$ splňuje*

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

***Souřadnicemi vektoru** $z \in V_n$ **v bázi** $\mathcal{X}$ nazveme uspořádanou ntici (sloupcový vektor[64])*

$$(z)_{\mathcal{X}} := \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in T^{n,1} \,.$$

*Číslo $\alpha_i \in T$ je **itá souřadnice vektoru** z **v bázi** $\mathcal{X}$, často značíme*[65]

$$x_i^{\#}(z) := \alpha_i.$$

Zdůrazněme, že pojem *souřadnice v bázi* je opravdu korektně definován. I když tím jen opakujeme důkaz Věty 2.70, 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 (Zkuste si to sami **dokázat**)!

(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 2.72 (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 $\mathcal{X}$.*

[63] Proč nutně? Nechť se každý zamyslí nad tím, jaké axiomy a jejich důsledky jsme k provedeným úpravám vlastně potřebovali...

[64] Připomínáme, že na sloupcový vektor $T^{n,1}$ můžeme také dle potřeby nahlížet jako na n**tici** z T^n, tj. $(z)_{\mathcal{X}} = (\alpha_1, \ldots, \alpha_n)$.

[65] Toto $x_i^{\#}$ nazýváme ***itý souřadnicový funkcionál v bázi*** $\mathcal{X}$.

1. *Hledáme ntici koeficientů $\alpha_1, \dots, \alpha_n \in T$ takovou, že příslušná lineární kombinace prvků báze je rovna vektoru z.*

2. *Koeficienty $\alpha_1, \dots, \alpha_n \in T$ 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 $\mathcal{X} = (x_1, \dots, x_n)$ je báze, musí existovat právě jedno řešení $(\alpha_1, \dots, \alpha_n)$ této soustavy – a to jsou hledané souřadnice vektoru z v bázi $\mathcal{X}$.*

Příklad 2.73. *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*

$$z = ae_1 + be_2 + ce_3\,.$$

A souřadnice obecného vektoru ve standardní bázi splňují

$$z = (a, b, c) \quad \Rightarrow \quad (z)_{\mathcal{E}_3} = (a, b, c)\,.$$

Příklad 2.74. *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 2.72.

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[66]*:*

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

$$\sim \left(\begin{array}{ccc|c} 1 & 1 & 0 & 2a-b \\ 0 & 1 & 0 & a-2b+c \\ 0 & 0 & 1 & b-a \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 0 & a+b-c \\ 0 & 1 & 0 & a-2b+c \\ 0 & 0 & 1 & b-a \end{array}\right)\,,$$

[66] 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.

s výsledkem $(\alpha, \beta, \gamma) = (a + b - c, a - 2b + c, b - a)$. *Tedy*

$$z = (a + b - c)x_1 + (a - 2b + c)x_2 + (-a + b)x_3$$

s souřadnice obecného vektoru v bázi $\mathcal{X}$ *splňují*

$$z = (a, b, c) \quad \Rightarrow \quad (z)_{\mathcal{X}} = (a + b - c, a - 2b + c, -a + b)\,.$$

Tedy například pro vektor $v = (4, 2, 3)$ *máme*

$$(v)_{\mathcal{X}} = (4 + 2 - 3, 4 - 2 \cdot 2 + 3, -4 + 2) = (3, 3, -2).$$

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*

$$\langle \mathbb{A}_{1:}, \ldots, \mathbb{A}_{m:}\rangle = \langle \mathbb{B}_{1:}, \ldots, \mathbb{B}_{m:}\rangle.$$

[1] Zkuste sami formulovat ke každé úpravě (G1)–(G3) takovou úpravu, která vede zpátky k původní matici.

[2] Tedy je prostě přestat psát.

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.

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

$$\langle \mathbb{A}_{1:}, \ldots, \mathbb{A}_{m:} \rangle = \langle \mathbb{A}_{1:}, \ldots, \mathbb{A}_{k:} \rangle$$

(ze souboru lze odebrat nulový vektor (obsahuje-li jej) 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 1.26 pomocí $1 \leq j_1 < j_2 < \cdots < j_k$ 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].

- $j_1$ní složka lineární kombinace závisí pouze na $\alpha_1 \mathbb{A}_{1:}$ (v prvním nenulovém sloupci jsou totiž kromě prvního řádku samé nuly). Jelikož v matici platí $\mathbb{A}_{1j_1} \neq 0$ 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

$$\alpha_1 \mathbb{A}_{1:} + \cdots + \alpha_{\ell-1} \mathbb{A}_{(\ell-1):} + \alpha_\ell \mathbb{A}_{\ell:}$$

[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.

[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.

(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 $h(\mathbb{A}) = k$. □

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.

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 $x_1, \dots x_m \in T^n$ spočítat $\dim\langle x_1, \dots, x_m\rangle$, 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 $y, x_1, \dots, x_m \in T^n$. Potřebujeme-li rozhodnout, zda

   $$y \in \langle x_1, \dots, x_m\rangle,$$

   uvědomíme si, že toto platí právě tehdy, když

   $$\langle x_1, \dots, x_m\rangle = \langle x_1, \dots, x_m, y\rangle.^{7}$$

   Jelikož se jedná o dva podprostory, které jsou v inkluzi, platí toto právě tehdy, když

   $$\dim\langle x_1, \dots, x_m\rangle = \dim\langle x_1, \dots, x_m, y\rangle.$$

   Tedy ověříme, zda hodnost matice, jejíž řádky jsou vektory $x_1, \dots, x_m$, je stejná jako hodnost matice, ve které je navíc přidán řádek y.

4. **Ověření rovnosti lineárních obalů:**
   Jsou dány $x_1, \dots, x_r, y_1, \dots, y_s \in T^n$. Potřebujeme-li ověřit, zda

   $$\langle x_1, \dots, x_r\rangle = \langle y_1, \dots, y_s\rangle,$$

[7] Jedna implikace plyne z Pozorování 2.32. Laskavý čtenář nechť se sám zamyslí nad implikací opačnou.

vzpomeneme si na Pozorování 2.68, podle kterého jsou tyto dva lineární obaly rovny právě tehdy, když

$$\dim\langle x_1,\dots,x_r\rangle = \dim\langle y_1,\dots,y_s\rangle = \dim\langle x_1,\dots,x_r,y_1,\dots,y_s\rangle.$$

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*

$$y \in \langle x_1,\dots,x_m\rangle \Leftrightarrow \exists \alpha_1 \dots \alpha_m \in T : y = \sum_{i=1}^{m} \alpha_i x_i \tag{3.2}$$

ověřit i přímo z definice, přes řešitelnost soustavy lineárních rovnic v neznámých $\alpha_1 \dots \alpha_m \in T$ (analogicky k Algoritmu 2.72).

Tyto dva různé postupy důrazně rozlišujme!

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 $\alpha_1,\dots,\alpha_n \in T$.*

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...

[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!

Následující věta pojednává 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*

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

Důkaz. Uvažujme rovnici

$$\alpha_1 \mathbb{A}_{:1} + \dots \alpha_n \mathbb{A}_{:n} = \theta,$$

díky vlastnostem maticového násobení (viz Věta 2.39) vlastně řešíme rovnici

$$\mathbb{A} \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \theta,$$

což lze maticově zapsat ve formě $(\mathbb{A}|\theta)$. Za pomoci Tvrzení 3.5 obdržíme, že tato soustava bude mít po GEMu právě $k := h(\mathbb{A})$ nenulových řádků.

$$(\mathbb{A}|\theta) \sim \left(\begin{array}{ccccccccccccc|c} 0 & \cdots & 0 & b_{1j_1} & \cdots & * & * & * & \cdots & * & * & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 & b_{2j_2} & * & \cdots & * & * & \cdots & 0 \\ \vdots & & & \vdots & & & \vdots & & \ddots & & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & b_{kj_k} & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots & & & \vdots & & & & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right),$$

kde indexům $j_1, \dots j_k$ odpovídají hlavní sloupce. Snadno ukážeme, že odpovídající sloupce původní matice $\mathbb{A}_{:j_1}, \dots \mathbb{A}_{:j_k}$ jsou lineárně nezávislé. Uvažujme rovnici

$$\alpha_{j_1} \mathbb{A}_{:j_1} + \dots \alpha_{j_k} \mathbb{A}_{:j_k} = \theta,$$

potom po maticovém zápisu této soustavy a aplikací stejných GEM operací jako dříve obdržíme soustavu

$$(\mathbb{A}_{:j_1}, \dots \mathbb{A}_{:j_k}|\theta) \sim \left(\begin{array}{cccc|c} b_{1j_1} & * & \cdots & * & 0 \\ 0 & b_{2j_2} & \cdots & * & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & b_{kj_k} & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \end{array}\right).$$

[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“.

Po vynechání posledních $n-k$ nulových řádků, získáme soustavu, která je v horním stupňovitém tvaru, kde právě poslední slupec je jediný vedlejší. Proto existuje právě jedno řešení a to $\alpha_{j_1} = \ldots = \alpha_{j_k} = 0$.

Z definice hodnosti a transpozice platí vztah $h(\mathbb{A}^T) = \dim\langle \mathbb{A}_{:1}, \ldots, \mathbb{A}_{:n}\rangle$. My jsme však právě zjistili, že existuje alespoň $k = h(\mathbb{A})$ lineárně nezávislých sloupců matice $\mathbb{A}$. Nutně tedy pro libovolnou matici $\mathbb{A}$ platí $h(\mathbb{A}) = k \leq h(\mathbb{A}^T)$. Aplikací tohoto vztahu na matici $\mathbb{A}^T$ konečně obdržíme

$$h(\mathbb{A}) \leq h(\mathbb{A}^T) \leq h\left((\mathbb{A}^T)^T\right) = h(\mathbb{A}).$$

□

Tato věta vlastně říká, že jsme klidně mohli definovat hodnost jinak (ale ekvivalentně!), a to jako dimenzi lineárního obalu souboru *sloupců* matice $\mathbb{A}$. Z toho také plyne následující tvrzení, které je triviální aplikací Důsledku Steinitzovy věty 2.51 (neboli tvrzení, že dimenze nemůže být větší, než počet generátorů).

Důsledek 3.8. *Nechť $\mathbb{A} \in T^{m,n}$. Potom $h(\mathbb{A}) \leq \min\{m, n\}$.*

V následující kapitolce využijeme, že hodnost součinu matic můžeme jednoduše odhadnout hodnostmi jich obou

Věta 3.9. *Je-li $\mathbb{A} \in T^{m,n}$ a $\mathbb{B} \in T^{n,p}$, potom*

$$h(\mathbb{AB}) \leq \min\left\{h(\mathbb{A}), h(\mathbb{B})\right\}.$$

Důkaz. Díky Větě 2.39 víme, že řádky matice $\mathbb{AB}$ jsou lineárními kombinacemi řádků matice $\mathbb{B}$ a tedy

$$\{(\mathbb{AB})_{1:}, (\mathbb{AB})_{2:}, \ldots (\mathbb{AB})_{m:}\} \subseteq \langle \mathbb{B}_{1:}, \ldots, \mathbb{B}_{n:}\rangle.$$

Z Pozorování 2.32 přímo obdržíme

$$\langle(\mathbb{AB})_{1:}, (\mathbb{AB})_{2:}, \ldots (\mathbb{AB})_{m:}\rangle \subseteq \langle \mathbb{B}_{1:}, \ldots, \mathbb{B}_{n:}\rangle$$

a tedy $h(\mathbb{AB}) \leq h(\mathbb{B})$.

Pro dokončení důkazu využijeme Větu 3.7 a předchozího kroku:

$$h(\mathbb{AB}) = h\left((\mathbb{AB})^T\right) = h\left(\mathbb{B}^T\mathbb{A}^T\right) \leq h(\mathbb{A}^T) = h(\mathbb{A}).$$

□

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 3.10. *V dalším textu budeme s oblibou pro zkrácení zápisů používat praktický symbol,* ***Kroneckerovo delta****, definovaný předpisem:*

$$\delta_{ij} = \begin{cases} 1, & \text{pro } i = j, \\ 0, & \text{jinak.} \end{cases}$$

Definice 3.11. ***Jednotkovou maticí*** *ntého řádu*[11] *rozumíme čtvercovou matici* $\mathbb{E} \in T^{n,n}$ *splňující*

$$\mathbb{E}_{ij} = \delta_{ij}\,, \quad i, j \in \hat{n}\,.$$

Pokud chceme zdůraznit rozměry této matice, píšeme $\mathbb{E}_n$ *namísto* $\mathbb{E}$.

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* $(\mathbb{A}_{11}, \mathbb{A}_{22}, \ldots, \mathbb{A}_{nn}) \in T^n$.

Pozorování 3.12. *Pokud* $\mathbb{A} \in T^{m,n}$, $\mathbb{E}_n \in T^{n,n}$ *a* $\mathbb{E}_m \in T^{m,m}$, *pak* $\mathbb{A}\mathbb{E}_n = \mathbb{A} = \mathbb{E}_m\mathbb{A}$.

Speciálně: pro $m = n$ *máme* $\mathbb{A}\mathbb{E}_n = \mathbb{A} = \mathbb{E}_n\mathbb{A}$

Tedy jednotková matice $\mathbb{E}_n$ 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 3.13. *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.

[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.

Věta 3.14. *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

$$\mathbb{A}\mathbb{B}_1 = \mathbb{B}_1\mathbb{A} = \mathbb{E} \quad \text{a současně} \quad \mathbb{A}\mathbb{B}_2 = \mathbb{B}_2\mathbb{A} = \mathbb{E}.$$

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. □

Přímo z definice plyne následující pozorování.

Pozorování 3.15. *Je-li $\mathbb{B}$ inverzní matice k $\mathbb{A}$, potom je $\mathbb{A}$ inverzní maticí k $\mathbb{B}$ a tedy $\mathbb{A}^{-1}$ je regulární matice a*

$$(\mathbb{A}^{-1})^{-1} = \mathbb{A}.$$

Věta 3.16. *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. Ukážeme, 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 $(\mathbb{A}\mathbb{B})^{-1} = \mathbb{B}^{-1}\mathbb{A}^{-1}$. □

Věta 3.17. *Nechť $\mathbb{A} \in T^{n,n}$ je regulární, potom $\mathbb{A}^T$ je také regulární a platí*

$$(\mathbb{A}^T)^{-1} = (\mathbb{A}^{-1})^T.$$

Důkaz. Opět dokážeme přímým dosazením. Ukážeme, že $(\mathbb{A}^{-1})^T$ je opravdu inverzní k matici $\mathbb{A}^T$, přitom využijeme jen definice inverzní matice a vlastnosti transpozice. Protože

$$\mathbb{A}^T(\mathbb{A}^{-1})^T = (\mathbb{A}^{-1}\mathbb{A})^T = \mathbb{E}^T = \mathbb{E}$$

a analogicky

$$(\mathbb{A}^{-1})^T\mathbb{A}^T = (\mathbb{A}\mathbb{A}^{-1})^T = \mathbb{E}^T = \mathbb{E}\,,$$

je podle definice matice $\mathbb{A}^T$ regulární a platí $(\mathbb{A}^T)^{-1} = (\mathbb{A}^{-1})^T$. □

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]:

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

$$\big(\mathbb{P}_i(\alpha)\big)^{-1} = \mathbb{P}_i(\alpha^{-1}).$$

[14] S využitím definice maticového násobení a bez jakýchkoli obav z dosazování obecných matic!

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 3.18. *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 $\mathbb{P}_1, \ldots, \mathbb{P}_n \in T^{m,m}$ (každá z nich je nějakého z výše uvedených tří typů). Tedy $\mathbb{B} = \mathbb{P}_n \ldots \mathbb{P}_1\mathbb{A}$. Protože součin regulárních matic je regulární matice, položíme $\mathbb{P} := \mathbb{P}_n \ldots \mathbb{P}_1$ a dostaneme tvrzení věty. □

Poznámka 3.19. *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]

[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.

O regulárních maticích

Jedna z klíčových vět této kapitoly nám řekne, s čím vším je *ekvivalentní* regularita čtvercové matice.

Věta 3.20. *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) ⇒ (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 $\mathbb{b} = (\beta_1, \ldots, \beta_n)$, odvodíme přepis rovnice (3.3) do jiného tvaru. Jelikož rovnost dvou vektorů implikuje rovnost jejich příslušných složek, přechází rovnice (3.3) v soustavu rovnic

$$\forall j \in \hat{n} : \Big(\sum_{i=1}^{n} \beta_i \mathbb{A}_{i:} \Big)_j = 0\,,$$

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 3.21. *Díky Větě 3.7 víme, že $h(\mathbb{A}) = h(\mathbb{A}^T)$, tedy platí také ekvivalence:*

$$\mathbb{A} \textit{ je regulární} \Leftrightarrow \textit{soubor sloupců matice } \mathbb{A} \textit{ je LN.}$$

Z Věty 3.20 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

$$\mathbb{P}\mathbb{A} = \mathbb{E}$$

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 $\mathbb{E} \sim \mathbb{P}\mathbb{E} = \mathbb{P} = \mathbb{A}^{-1}$, tedy hledaná inverze.

Algoritmus 3.22 (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 3.20 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 3.23. *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 3.24. *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. □

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.

Věta 3.25. *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. Uvažujme případ $\mathbb{A}\mathbb{B} = \mathbb{E}$, potom díky Větě 3.9 můžeme odhadovat

$$n = h(\mathbb{E}) = h(\mathbb{A}\mathbb{B}) \leq h(\mathbb{A}) \leq n.$$

Tedy $h(\mathbb{A}) = n$ a z Věty 3.20 víme, že $\mathbb{A}$ je regulární. Navíc

$$\mathbb{A}^{-1} = \mathbb{A}^{-1}\mathbb{E} = \mathbb{A}^{-1}\mathbb{A}\mathbb{B} = \mathbb{B}.$$

Druhý případ se udělá analogicky. □

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.

[16] Přeznačení koeficientů v soustavě rovnic $a_{ij} \to \alpha_{ij}$ a $b_i \to \beta_i$ by nikomu zkazit den nemělo.

Pozorování 3.26. *Množina S_0 všech řešení homogenní soustavy $\mathbb{A}\mathbb{x} = \theta$ je podprostor ve VP $T^{n,1}$.*

Následující hlavní výsledek budeme v celém kurzu titulovat „Frobeniova věta“[17], 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[18]. 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[19]. Současně lze narazit na různé varianty této věty, někde se jako její součást uvádí pouze bod (i), někde oba.

Věta 3.27 (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

$$h(\mathbb{A}) = h(\mathbb{A} \mid \mathbb{b}).$$

(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. 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**. V této kapitole dokážeme pouze bod (i). Bod (ii) dokážeme později, v kapitole o lineárních zobrazeních, na konci Podkapitoly 5.4.

[17] Řekněme, že je to důsledek takové naší lokální tradice.

[18] Pan Frobenius toho dokázal poměrně hodně.

[19] Důvody mohou být společná historie a kulturní vliv (Frobenius u nás, případně Kronecker–Capelli shodně v Rusku, Polsku a Maďarsku), připadně „fandění domácímu týmu“ (Rouché–Fontené ve Francii).

(i) **(⇒) :** 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 [20].

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 $h(\mathbb{A}) = h(\mathbb{A} \mid \mathbb{b})$.

(⇐) : Nechť $h(\mathbb{A}) = h(\mathbb{A} \mid \mathbb{b})$. Protože platí

$$\langle \mathbb{A}_{:1}, \ldots, \mathbb{A}_{:n} \rangle \subset\subset \langle \mathbb{A}_{:1}, \ldots, \mathbb{A}_{:n}, \mathbb{b} \rangle$$

a současně mají tyto podprostory v $T^{m,1}$ stejnou konečnou dimenzi, musí platit dle Důsledku 2.62, že

$$\langle \mathbb{A}_{:1}, \ldots, \mathbb{A}_{:n} \rangle = \langle \mathbb{A}_{:1}, \ldots, \mathbb{A}_{:n}, \mathbb{b} \rangle .$$

[20] Toto nechť si každý čtenář nechá důkladně projít hlavou.

Speciálně tedy

$$\mathbb{b} \in \langle \mathbb{A}_{:1}, \ldots, \mathbb{A}_{:n} \rangle,$$

a proto existují $y_1, \ldots, y_n \in T$ 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 $\mathbb{y} = (y_1, \ldots, y_n)^T$. Soustava $\mathbb{A}\mathbb{x} = \mathbb{b}$ tedy má řešení $\mathbb{y} \in S$.

□

Poznámka 3.28. *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*

$$\mathbb{x} = \mathbb{A}^{-1}\mathbb{b}\,.$$

Ctěného čtenáře si zde dovolujeme laskavě vyzvat k zopakování definice horního stupňovitého tvaru matice (Definice 1.26), 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 $1 \leq j_1 < j_2 < \cdots < j_h$.

$$\left(\begin{array}{ccccccccccccc|c}
0 & \cdots & 0 & \underbrace{\alpha_{1j_1}}_{\neq 0} & \cdots & * & * & \cdots & * & * & \cdots & * & * & \cdots & \beta_1 \\
0 & \cdots & 0 & 0 & \cdots & 0 & \underbrace{\alpha_{2j_2}}_{\neq 0} & \cdots & * & * & \cdots & * & * & \cdots & \beta_2 \\
0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & \underbrace{\alpha_{3j_3}}_{\neq 0} & \cdots & * & * & \cdots & \beta_3 \\
\vdots & & & \vdots & & & \vdots & & & \vdots & \ddots & & \vdots & & \vdots \\
0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & \underbrace{\alpha_{hj_h}}_{\neq 0} & \cdots & \beta_h \\
0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\
\vdots & & & \vdots & & & \vdots & & & \vdots & & & \vdots & & \vdots \\
0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0
\end{array}\right)$$

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 3.29 (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*[21]*.*
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*[22]*, který generuje S_0.*

[21] V případě standardní báze tedy samozřejmě platí $(t_1, t_2, \ldots, t_{n-h}) \in \langle (1, 0, 0, \ldots, 0, 0), (0, 1, 0, \ldots, 0, 0), \ldots, (0, 0, 0, \ldots, 0, 1) \rangle$.

[22] Lineární nezávislost tohoto souboru si dobře rozmyslete.

Příklad 3.30. *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:* $x_4 = 0$, $x_2 = -\frac{1}{2}$, $x_1 = -\frac{1}{2}$.
- *Při volbě $(x_3, x_5) = (0, 1)$ dopočítáme:* $x_4 = -\frac{3}{2}$, $x_2 = \frac{7}{4}$, $x_1 = -\frac{33}{4}$.
- *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.

Věta 3.31. *Nechť $\mathbb{A} \in T^{m,n}$ a*

$$\mathbb{A} \sim \begin{pmatrix} \mathbb{E}_k & \mathbb{B} \\ \Theta & \Theta \end{pmatrix},$$

kde $\mathbb{E}_k \in T^{k,k}$ je jednotková matice, $\mathbb{B} \in T^{k,n-k}$ a symboly Θ značí nulové matice příslušných rozměrů[23]*. Potom řádky matice*

$$(-\mathbb{B}^T \;\; \mathbb{E}_{n-k}) \in T^{n-k,n},$$

kde $\mathbb{E}_{n-k} \in T^{n-k,n-k}$ je jednotková matice, tvoří bázi prostoru řešení S_0.

[23] Jedna je typu $(m-k) \times k$, druhá je typu $(m-k) \times (n-k)$.

Důkaz. Řešme dle Algoritmu 3.29 soustavu s maticí

$$\begin{pmatrix} \mathbb{E}_k & \mathbb{B} \\ \Theta & \Theta \end{pmatrix}.$$

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

$$(-\mathbb{B}^T \ \mathbb{E}_{n-k}) \in T^{n-k,n}.$$

Alternativně lze využít blokového násobení matic (viz Definice 3.51 v dodatku na konci této kapitoly). Pak dostáváme

$$\begin{pmatrix} \mathbb{E}_k & \mathbb{B} \\ \Theta & \Theta \end{pmatrix} \begin{pmatrix} -\mathbb{B} \\ \mathbb{E}^T_{n-k} \end{pmatrix} = \begin{pmatrix} -\mathbb{E}_k\mathbb{B} + \mathbb{B}\mathbb{E}^T_{n-k} \\ \Theta \end{pmatrix} = \begin{pmatrix} -\mathbb{B} + \mathbb{B} \\ \Theta \end{pmatrix} = \Theta.$$

□

Příklad 3.32. *Ještě jednou si vyřešíme soustavu z Příkladu 3.30, pro neznámé* $(x_1, x_2, x_3$

$$\mathbb{A} = \left(\begin{array}{ccccc|c} 1 & 3 & 2 & 0 & 3 & 0 \\ 1 & 1 & 1 & -1 & 5 & 0 \\ 2 & 8 & 5 & 3 & 7 & 0 \\ 3 & 9 & 6 & 2 & 12 & 0 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 1/2 & 0 & 33/4 & 0 \\ 0 & 1 & 1/2 & 0 & -7/4 & 0 \\ 0 & 0 & 0 & 1 & 3/2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Prohozením třetího a čtvrtého sloupce dostaneme soustavu ve speciálním tvaru, kde neznámé jsou $(x_1, x_2, x_4, x_3, x_5)$*:*

$$(\mathbb{E} \ \mathbb{B}) = \begin{pmatrix} 1 & 0 & 0 & 1/2 & 33/4 \\ 0 & 1 & 0 & 1/2 & -7/4 \\ 0 & 0 & 1 & 0 & 3/2 \end{pmatrix}$$

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 3.33 (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*[24] *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 3.34. *Soustavu s maticí uvedenou v předchozích příkladech doplníme o pravou stranu. Řádkovými úpravami GEM upravíme rozšířenou matici:*

$$\left(\begin{array}{ccccc|c} 1 & 3 & 2 & 0 & 3 & 3 \\ 1 & 1 & 1 & -1 & 5 & -2 \\ 2 & 8 & 5 & 3 & 7 & 13 \\ 3 & 9 & 6 & 2 & 12 & 11 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 1/2 & 0 & 33/4 & -3 \\ 0 & 1 & 1/2 & 0 & -7/4 & 2 \\ 0 & 0 & 0 & 1 & 3/2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

[24] 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* $(x_1, x_2, x$ *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 3.30 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.

Lemma 3.35. *Je-li* $P \subset\subset V$ *a* $x \in P$, *potom* $x + P = P$.

Důkaz. Ukážeme rovnost množin. Je-li $y \in x+P$ potom existuje $p \in P$ tak, že $y = x+p$. Tedy

$$y = \underbrace{x}_{\in P} + \underbrace{p}_{\in P} \in P.$$

Proto $x + P \subseteq P$.

Naopak každé $p \in P$ lze zapsat ve tvaru

$$p = \underbrace{x}_{\in P} + \underbrace{p - x}_{\in P} \in x + P.$$

Tedy i $P \subseteq x + P$.

□

Pozorování 3.36. *Nechť* $u, v, y_1, \ldots, y_k, z_1, \ldots, z_k \in T^n$, *kde soubory* $(y_1, \ldots, y_k)$ *a* $(z_1, \ldots, z_k)$ *jsou LN. Rovnost*

$$u + \langle y_1, \ldots, y_k\rangle = v + \langle z_1, \ldots, z_k\rangle \tag{3.5}$$

platí právě tehdy, když matice, jejíž řádky tvoří vektory

$$y_1, \ldots, y_k, z_1, \ldots, z_k, u - v$$

má hodnost rovnu k.

Důkaz.
($\Rightarrow$) : Platí-li (3.5), pak $u - v + \langle y_1, \dots, y_k \rangle = \langle z_1, \dots, z_k \rangle$. Z rovnosti rovnou plyne, že $u - v = u - v + \theta \in \langle z_1, \dots, z_k \rangle$. Navíc díky předchozímu lemmatu a první rovnosti v důkazu platí

$$\langle z_1, \dots, z_k \rangle = \underbrace{v - u}_{\in \langle z_1, \dots, z_k \rangle} + \langle z_1, \dots, z_k \rangle = \langle y_1, \dots, y_k \rangle,$$

neboli oba lineární obaly se rovnají. Celkově máme

$$\langle y_1, \dots, y_k \rangle = \langle y_1, \dots, y_k, z_1, \dots, z_k \rangle = \langle y_1, \dots, y_k, z_1, \dots, z_k, u - v \rangle$$

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, získáme

$$u - v \in \langle y_1, \dots, y_k \rangle,$$

tedy s pomocí předchozího lemmatu vyplyne

$$\langle y_1, \dots, y_k \rangle = u - v + \langle y_1, \dots, y_k \rangle.$$

Dále protože

$$\dim \langle y_1, \dots, y_k \rangle = \dim \langle z_1, \dots, z_k \rangle = \dim \langle y_1, \dots, y_k, z_1, \dots, z_k \rangle = k,$$

dostáváme z Pozorování 2.68 o rovnosti lineárních obalů rovnost

$$\langle y_1, \dots, y_k \rangle = \langle z_1, \dots, z_k \rangle.$$

Celkem máme

$$\langle z_1, \dots, z_k \rangle = \langle y_1, \dots, y_k \rangle = u - v + \langle y_1, \dots, y_k \rangle.$$

Nakonec si stačí opět uvědomit, že předchozí rovnost platí právě tehdy, když platí následující

$$u + \langle y_1, \dots, y_k \rangle = v + \langle z_1, \dots, z_k \rangle$$

□

Příklad 3.37. *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

$$S_1 = (\tfrac{1}{5}, \tfrac{2}{5}, 0, 0) + \langle (2, -1, 5, 0), (1, 2, 0, 5) \rangle,$$
$$S_2 = (0, 0, 0, -1) + \langle (0, -5, 5, -10), (3, 1, 5, 5) \rangle.$$

To, že se tyto množiny rovnají[25]*, ověříme výpočtem hodnosti matice sestavené podle Pozorování 3.36,*

$$\begin{pmatrix} 2 & -1 & 5 & 0 \\ 1 & 2 & 0 & 5 \\ 0 & -5 & 5 & -10 \\ 3 & 1 & 5 & 5 \\ \frac{1}{5} & \frac{2}{5} & 0 & 1 \end{pmatrix},$$

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 $V = T^n$.

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 3.27) 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 3.38. *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

$$x_1 \begin{pmatrix} \alpha_{11} \\ \alpha_{21} \\ \vdots \\ \alpha_{m1} \end{pmatrix} + x_2 \begin{pmatrix} \alpha_{12} \\ \alpha_{22} \\ \vdots \\ \alpha_{m2} \end{pmatrix} + \cdots + x_n \begin{pmatrix} \alpha_{1n} \\ \alpha_{2n} \\ \vdots \\ \alpha_{mn} \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_m \end{pmatrix}.$$

[25] 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“!

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 $\mathbb{b}$ (Pozorný čtenář si jistě vzpomene na Větu 2.39 o tom, že na součin dvou matic můžeme nahlížet jako na lineární kombinaci jejich řádků/sloupců!).*

Pozorování 3.39. *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[26]) je množina bodů v T^n, kterou si lze geometricky představit[27]. 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.*

Definice lineární variety

Pod pojmem *lineární varieta* budeme rozumět libovolný podprostor „posunutý“ z počátku θ o nějaký vektor.

Definice 3.40. *Neprázdnou množinu $W \subseteq V$ nazveme* ***lineární varietou*** *(případně pouze* ***varietou****), pokud existují $a \in V$ 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.*

[26] A co když jsou všechny α_{ij} v nějakém řádku nulové, co platí pak?
[27] Alespoň v omezené míře, že ano…

Věta 3.41. *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.

(iii) Máme-li $a, b \in V$ a $P, Q \subset\subset V$, potom pro dvě variety platí $a + P = b + Q$ právě tehdy, když $P = Q$ a zároveň $b - a \in P$.

Důkaz. (i) Nechť $W = b + Z(W)$. Pak pro libovolné $a \in W$ existuje $x \in Z(W)$ tak, že $a = b + x$. Odkud dostáváme, že $b - a = -x \in Z(W)$.

Za pomocí Lemmatu 3.35 obdržíme

$$b + Z(W) = (a + b - a) + Z(W) = a + (b - a + Z(W)) = a + Z(W).$$

(ii) Existují-li dva podprostory $P, Q \subset\subset V$ takové, že

$$W = a + P = a + Q,$$

dostaneme přičtením vektoru $-a$ k oběma stranám rovnosti ihned, že $P = Q$.

(iii) „$\Rightarrow$“ Z rovnosti variet speciálně platí $b \in a + P$. Proto existuje $p \in P$ tak, že $b = a + p$, z čehož plyne

$$b - a = p \in P.$$

Z předpokladu $a + P = b + Q$ plyne, že prvek $a = a + \theta$ z variety $a + P$ náleží také do variety $b + Q$. Díky předpokladu a bodu (i) získáme, že

$$a + P = b + Q = a + Q.$$

Rovnost $P = Q$ pak plyne plyne přímo z bodu (ii) o jednoznačnosti zaměření variety.

„$\Leftarrow$“ Za pomocí Lemmatu 3.35 obdržíme

$$a + P = b + \underbrace{a - b}_{\in P} + P = b + P = b + Q.$$

□

Definice 3.42. *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 3.43. *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 3.40 a 3.42. 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 3.44. *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 3.45. *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, kterou si označme $\mathbb{Y} \in T^{n,k}$, musí platit
   $$\mathbb{A}\mathbb{Y} = \Theta \in T^{n-k,k}\,,$$ [28]
   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 3.27 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
   $$\mathbb{A}\mathbb{a} = \mathbb{b}\,.$$

[28] Uvědomit si, jakých rozměrů jsou používané matice, nikdy neuškodí.

Vztah $h(\mathbb{A}) = n - \dim M$ plyne přímo z Frobeniovy věty 3.27 a předchozích bodů v důkazu. □

Jednoduchý důsledek získáme použitím předchozí věty ve speciálním případě $\dim P = n - 1$.

Důsledek 3.46. *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 3.47. *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*

$$u \in W \Leftrightarrow \exists \alpha_1, \ldots, \alpha_k \in T:\ u = a + \sum_{i=1}^{k} \alpha_i a_i\,.$$

  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 3.47. Druhý směr převodu, **z parametrických rovnic na neparametrické**, se v podstatě řídí postupem důkazu Věty 3.45, heslovitě si jej tady ještě zopakujeme.

Algoritmus 3.48 (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 $(y_1, \ldots, y_k)$ a vyřešme homogenní soustavu $(\widetilde{\mathbb{Y}} \mid \theta)$ kde matice $\widetilde{\mathbb{Y}}$ obsahuje ve svých řádcích vektory $y_1, \ldots, y_k$.*

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 3.49. *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 3.50. *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

$$\begin{aligned} s_1 &= (2,3,2,1) - (1,2,1,0) = (1,1,1,1)\,, \\ s_2 &= (3,2,4,0) - (1,2,1,0) = (2,0,3,0)\,. \end{aligned}$$

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 3.48 vyřešíme homogenní soustavu s maticí

$$\left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 2 & 0 & 3 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 0 & -2 & 1 & -2 & 0 \end{array}\right). \tag{3.6}$$

Báze množiny řešení soustavy (3.6) 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* $\mathbb{R}^4$*:*

$$\begin{aligned} -y \quad &+ u = -2 \\ -3x + \; y + 2z \quad &= 1\,. \end{aligned}$$

3.6 Dodatky

Blokové násobení a algoritmy pro maticové násobení

Definice 3.51. *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

$$\mathbb{A}(\mathbb{B}_1\ \mathbb{B}_2\ \ldots\ \mathbb{B}_p) = (\mathbb{A}\mathbb{B}_1\ \mathbb{A}\mathbb{B}_2\ \ldots\ \mathbb{A}\mathbb{B}_p). \tag{3.7}$$

Uvažujme čtvercové matice $\mathbb{A}, \mathbb{B} \in T^{n,n}$. K výpočtu součinu $\mathbb{AB}$ podle definice potřebujeme n^3 operací (operací myslíme vynásobení dvou čísel, které je výpočetně náročnější než sčítání)[29]. Nedalo by se ušetřit?

Rekurzivní algoritmus násobení matic: Vychází z blokového násobení (Definice 3.51). 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 poloviční rozměrů (plus nějaké to sčítání, které zanedbáváme). Počet operací násobení označme $F(n)$, potom platí:[30]

$$\begin{aligned} F(n) =& 8F(n/2) = 8(8F(n/4)) = 8(8(8F(n/8))) = \cdots \\ =& 8^k F(n/2^k) = 8^k F(1) = 8^k = (2^k)^3 = \\ =& n^3. \end{aligned}$$

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

$$\begin{pmatrix} \mathbb{A}_1 & \mathbb{A}_2 \\ \mathbb{A}_3 & \mathbb{A}_4 \end{pmatrix} \begin{pmatrix} \mathbb{B}_1 & \mathbb{B}_2 \\ \mathbb{B}_3 & \mathbb{B}_4 \end{pmatrix} = \begin{pmatrix} \mathbb{X}_1 + \mathbb{X}_4 - \mathbb{X}_5 + \mathbb{X}_7 & \mathbb{X}_3 + \mathbb{X}_5 \\ \mathbb{X}_2 + \mathbb{X}_4 & \mathbb{X}_1 - \mathbb{X}_2 + \mathbb{X}_3 + \mathbb{X}_6 \end{pmatrix}.$$

Pro počet operací $F(n)$, kde opět pro jednoduchost předpokládáme $n = 2^k$, nyní dostáváme lepší odhad:

$$\begin{aligned} F(n) =& 7F(n/2) = 7(7F(n/4)) = 7(7(7F(n/8))) = \cdots \\ =& 7^k F(n/2^k) = 7^k F(1) = 7^k = 7^{\log_2 n} = \\ =& n^{\log_2 7} \cong n^{2{,}807}. \end{aligned}$$

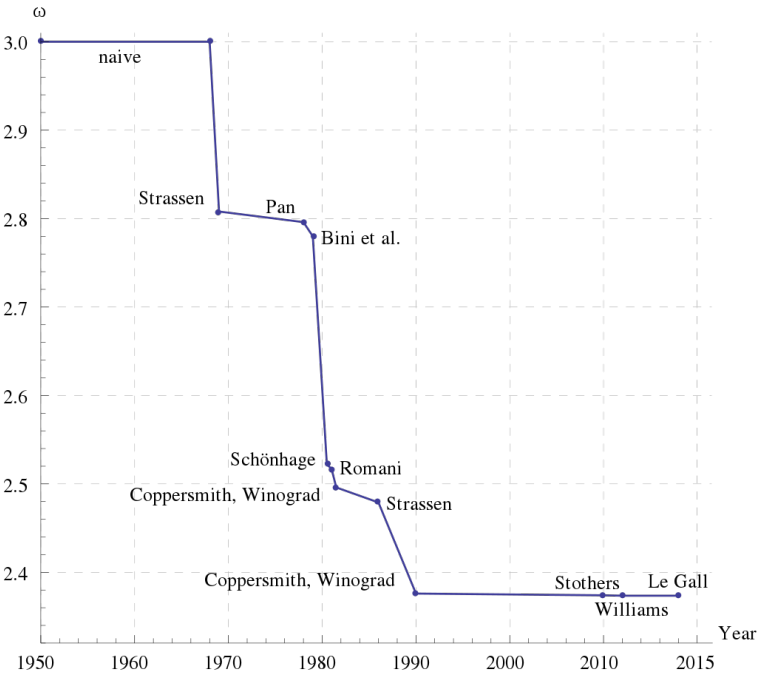
[31]

Strassenův algoritmus se běžně používá pro násobení velkých matic. Existují sice asymptoticky rychlejší algoritmy pro maticové násobení, nicméně jejich výhoda by se projevila až pro extrémně velké matice (které ani nelze v počítači reprezentovat). V současnosti je asymptoticky nejrychlejší algoritmus od Françoisa Le Galla (publ. 2014), který počítá s přibližně $\mathbf{n^{2{,}3728639}}$ operacemi.

[29] Je to takový přibližný odhad, součin $\mathbb{AB}$ má n^2 prvků, pro každý z nich počítáme sumu n sčítanců a pro každý z nich potřebujeme jedno násobení.

[30] 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.

[31] Proč předposlední rovnost $7^{\log_2 n} = n^{\log_2 7}$ vůbec platí? Schválně si trochu procvičte úpravy mocnin.



Obrázek 3.1: Výpočetní složitosti algoritmů pro maticové násobení [zdroj: wikipedia.org]

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 01000110. To může vést k nedorozumění[4], nepochopení textu apod., přesto adresát nemá šanci poznat, že se

[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“!

něco pokazilo, natož pak co přesně se pokazilo.

Lineární 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.

Lineární kódy používáte prakticky denně při práci s PC, či mobilem. Nějaké příklady užití zmíníme v sekci Dodatky 4.5. Student Fitu je potká například ještě v BI-JPO[5] či MI-BKO.[6]

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*[7]*. Prvky abecedy nazýváme* ***písmena*** *(příp.* ***znaky****) a jakýkoli řetězec n písmen*

[5] Jednotky počítače, zimní semestr druhého ročníku bakalářského studia.

[6] Bezpečnostní kódy, zimní semestr prvního ročníku magisterského studia.

[7] 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.

$a_1 a_2 \cdots a_n$, *kde* $n \in \mathbb{N}_0$, *nazýváme* ***slovo*** *délky* n. *Je-li* $n = 0$, *mluvíme o* ***prázdném slově***.

Množinu všech (konečných) slov nad abecedou[8] $\mathcal{A}$ *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[9] a dokonce i když vezmeme sjednocení všech abeced všech jazyků[10], 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.

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*[11]*, 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!*

[8] Divný výraz „slovo nad abecedou $\mathcal{A}$“ znamená „slovo, jehož písmena jsou z abecedy $\mathcal{A}$“. Se to takto prostě vžilo.

[9] Dokonce i v němčině jsou všechna slova konečná.

[10] Klidně i včetně klingonštiny.

[11] Zamýšlení obecně doporučujeme!

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 *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*[12]*, obecně ale v teorii samoopravovacích kódů pracujeme s předpokladem, že* ***výskyt méně chyb je pravděpodobnější než výskyt více chyb****. Tento*[13] *předpoklad ospravedlňuje adresáta, který slovo* **1**10**1**10**1**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 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[14] *ale dokonce i opravit*[15]*, 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[16]. 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, musíme 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**.

[12] Když si např. připustíme, že se stane v devíti bitovém slově až devět chyb, je možné cokoli, kód nekód.

[13] Imho rozumný.

[14] „Ha! Něco je špatně!“

[15] „Ha! Něco je špatně a navíc vím kde a co!“

[16] Toto si prosím rozmyslete a pochopte alespoň na úrovni „když n je 5, tak chápu, proč kód objevuje 4 chyby a opravuje jen 2“.

Příklad 4.3 (Paritní kód)**.** *Obecně paritní kód funguje takto: Mějme n bitové slovo $b_1b_2\cdots b_n \in \mathcal{A}_2^n$. Toto slovo zakódujeme tak, že k němu přidáme jeden bit b_{n+1} tak, aby počet jedniček ve výsledném slově $b_1b_2\cdots b_nb_{n+1}$ 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[17]. Předně jsme si zatím neřekli, co je to vlastně to kódování. Už v 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***[18]*. Obor hodnot tohoto zobrazení $H_\kappa \subseteq \mathcal{B}^+$ nazýváme* ***kód****, označujeme jej K a libovolné slovo z $K = H_\kappa$ nazýváme* ***kódové slovo****.*

Zobrazení přirozeně rozšiřujeme na slova z $\mathcal{A}^+$ takto: buď $u = u_1u_2\cdots u_n \in \mathcal{A}^n$ slovo délky n s písmeny $u_i \in \mathcal{A}$. Potom

$$\kappa(u) = \kappa(u_1)\kappa(u_2)\cdots\kappa(u_n).$$

Dále budeme uvažovat pouze ty kódy, které mají **alespoň dva prvky**.[19]

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*

[17] Definice příkladem je sice pedagogicky vhodná, ale z pohledu matematiky by byla hanba, u takové definice zůstat!

[18] To divné písmenko κ je řecká kappa.

[19] Rozmyslete si, že s jednoprvkovým kódem bychom ztratili veškerou infomaci o původním slově.

vzali množinu 3bitových písmen[20]

$$\mathcal{A}_2^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$$

a za abecedu $\mathcal{B}$ pak binární abecedu[21]*. 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 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*[22] *z vektorového prostoru $\mathbb{Z}_2^n$. Když tedy přistoupíme*[23] *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:*

$$\kappa(b_1b_2\cdots b_n) = b_1b_2\cdots b_nb_{n+1}, \quad \text{kde } b_{n+1} = b_1 + b_2 + \cdots + b_n.$$

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 $\kappa(110) = 1100$.

[20] Že říkáme 3písmenným slovům písmena? Je to konečná alespoň dvouprvková množina? Je! Abeceda je každá konečná alespoň dvouprvková množina!

[21] Kódová slova mají všechna délku 9, binárních slov délky 9 je celkem $2^9 = 512$. Z pochopitelných důvodů je zde nebudeme vypisovat.

[22] 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!

[23] Kdo na to nepřistoupí, bude zejména v příští kapitole trpět.

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[24]. 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:

Definice 4.7. *Pro dvě slova $u = u_1u_2\cdots u_n$ a $v = v_1v_2\cdots v_n$ 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

$$d(010010010, 110110110) = 3,$$

[24] Pokud děláte překlepy, tak máte celkem dobrou představu, co se může stát.

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[25]. 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[26]. 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 nedostaneme na jiné kódové slovo tím, že se v něm přepíše t písmen[27].

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 nám bude stačit základní pochopení. Dekódování bude probíhat v zásadě takto[28]: Předpokládejme, že používáme kód K a přijmeme slovo u (toto slovo může a nemusí obsahovat chyby).

[25] Zkuste si rozmyslet, že Hammingova vzdálenost dvou kódových slov paritního kódu je vždy sudá.

[26] „Každý řetěz je silný jen tak, jak je silný jeho nejslabší článek.“ *Arthur Conan Doyle, J. Watson – Údolí strachu*

[27] To vlastně znamená, že kód objevuje KAŽDOU možnou chybu v libovolných t písmenech libovolného kódového slova.

[28] Na konkrétních příkladech už jsme to vlastně předvedli výše, aniž bychom tomu říkali dekódování.

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*[29]*. 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*[30]*.*

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.

Pokud obě definice dáme dohromady, získáme:

[29] Zkuste si rozmyslet, že další nejbližší kódové slovo má vzdálenost 3.

[30] 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.

Pozorování 4.12. *Je-li $\mu(K) = n$, potom kód K objevuje $n-1$ (a menší) chyby a opravuje $\lfloor \frac{n-1}{2} \rfloor$ (a menší) chyby.*

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[31].

Dva výše uvedené příklady by mohly 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 tříbitových 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.

[31] Ne že by to nešlo udělat, ale vyžadovalo by to trochu sofistikovanější metody, kterými si jednoduchou lineární algebru nebudeme kazit (viz např. pojem entropie)).

Definice 4.13. *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 $\varphi : \mathcal{B}^k \to K$.*

Když mezi dvěma konečnými množinami existuje bijekce, mají tyto dvě množiny nutně stejně prvků[32]. Předchozí definici bychom tedy mohli ekvivalentně přepsat tak, že kód $K \subseteq \mathcal{B}^n$ 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 $K \subseteq \mathbb{Z}_2^n$ 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[33] (jsou vždy na začátku) a ty, které jsou kontrolní (jsou vždy až za těmi informačními). To je zejména z pohledu implementace velmi výhodné[34]. Chceme-li například kódovat tříbitová slova $000, 001, \ldots, 111$ 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 4.13. 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 4.14. *Mějme kód $K \subseteq \mathcal{B}^n$ s k informačními a $n-k$ kontrolními znaky. Lze-li bijekci φ z Definice 4.13 zvolit tak, že pro každé $u \in \mathcal{B}^k$ existuje $v \in \mathcal{B}^{n-k}$ takové, že*

$$\varphi(u) = uv \in K,$$

[32] 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.

[33] Pojem „nést informaci“ jsme si nedefinovali, ale věříme, že laskavý čtenář intuitivně tuší, co tím myslíme.

[34] 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.

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.

Věta 4.15 (Singletonův odhad)**.** *Mějme kód $K \subseteq \mathcal{B}^n$, potom*

$$\#K \leq (\#\mathcal{B})^{n-\mu(K)+1}, \tag{4.1}$$

kde $\#$ značí počet prvků v množině.

Speciálně: je-li $K \subseteq \mathcal{B}^n$ kód s k informačními znaky, platí pro jeho minimální vzdálenost

$$\mu(K) \leq n - k + 1. \tag{4.2}$$

Důkaz. Označme si $d := \mu(K)$ a uvažujme zkrácený kód

$$K' := \{u_1 u_2 \dots u_{n-d+1} \in \mathcal{B}^{n-d+1}, \text{ takové, že } u_1 \dots u_n \in K\},$$

který vznikne ze slov kódu K vynecháním posledních $d-1$ znaků.

Mějme libovolná dvě různá kódová slova $u, v \in K$. Jelikož je $\mu(K) = d$, musí se tato slova lišit alespoň v d znacích, přičemž alespoň jeden rozdíl musí být v prvních $n-d+1$ znacích. Proto se nutně liší i zkrácená slova $u_1 \dots u_{n-d+1}$ a $v_1 \dots v_{n-d+1}$.

Tedy ke každému slovu z K existuje právě jedno slovo z K'. Proto má K stejně prvků jako K', kterých je nejvýše tolik, kolik je slov v $\mathcal{B}^{n-d+1}$. Z čehož plyne nerovnost (4.1).

Konečně ve speciálním případě, kdy kód má k informačních bitů máme

$$(\#\mathcal{B})^k = \#K \leq (\#\mathcal{B})^{n-\mu(K)+1}.$$

Ze získáné nerovnosti již přímočaře plyne požadovaná nerovnost (4.2).

□

Pro paritní kód, který má jediný kontrolní znak, je hranice „počet kontrolních znaků + 1“ tedy dosaženo[35], 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.

[35] Takové kódy, pro které platí v (4.2) rovnost, se nazývají MDS kódy (viz část Dodatky 4.5).

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

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

Když se tedy smíříme s tímto ztotožněním slova a vektoru, můžeme říci, 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[36].

Definice 4.16. *Podmnožinu K vektorového prostoru $\mathbb{Z}_p^n$ nazveme **lineární** (n,k)-**kód**[37], jestliže je K podprostor dimenze k.*

*Nechť $k \in \{1, 2, \ldots, n-1\}$[38]. 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.*

[36] Skutečně, viz Věta 3.45, 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 $\mathbb{b} = \theta$.

[37] V jiných materiálech lze nalézt značení $[n,k]$-kód, respektive $[n,k,l]$-kód, pokud má kód minimální vzdálenost l.

[38] Lineární (n,k)-kódy pro $k \in \{0, n\}$ jsou pro nás nezajímavé a nebudeme se jimi zabývat. Laskavý čtenář se jistě sám zamyslí, proč tomu tak je.

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[39] 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[40] 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 K a množinou $\mathbb{Z}_p^k$. To dle Definice 4.13 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 4.17. *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 $a = a_1 a_2 \cdots a_k \in \mathbb{Z}_p^k$. Definujeme zobrazení $\varphi : \mathbb{Z}_p^k \to \mathbb{Z}_p^n$ předpisem

$$\varphi(a) := \left((a_1\ a_2\ \cdots\ a_k) \cdot G_K\right)^T,$$

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[41]. □

[39] Použijeme-li značení z Frobeniovy věty 3.27, je K vlastně množina řešení homogenní soustavy značená S_0.

[40] Rozmyslete si, jak funguje maticové násobení!

[41] A my už dávno víme, že přiřazení „vektor ↔ jeho souřadnice ve zvolené bázi“ je vzájemně jednoznačné.

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 4.18 (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/vektor 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[42] *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[43] *a abychom získali nějakou generující, stačí najít bázi řešení homogenní soustavy s touto maticí, tedy soustavy*

$$\left(\begin{array}{ccccc|c} 1 & 1 & 1 & \cdots & 1 & 0. \end{array}\right)$$

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:

[42] Ve Frobeniově větě značená jako S_0.

[43] A označit ji H_K bylo tedy nanejvýš prozíravé!

Příklad 4.19. *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, $b_1b_2\dots b_9$ je kódové slovo jestliže je řešením následující homogenní soustavy*[44]

$$\left(H_{K^3} \mid \theta\right) = \left(\begin{array}{ccccccccc|c} 1&0&0&1&0&0&0&0&0&0\\ 0&1&0&0&1&0&0&0&0&0\\ 0&0&1&0&0&1&0&0&0&0\\ 0&0&0&1&0&0&1&0&0&0\\ 0&0&0&0&1&0&0&1&0&0\\ 0&0&0&0&0&1&0&0&1&0 \end{array}\right).$$

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.

Příklad 4.20. *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:*

$$00000, 10021, 20012, 00110, 00220, 10101, 20122, 10211, 20202.$$

[44] 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.

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 3.45: 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 4.21. *Lineární (n, k)-kód je systematický právě tehdy, když generující matici* ***lze volit*** *ve tvaru*

$$G_K = \begin{pmatrix} \mathbb{E}_k & \mathbb{A} \end{pmatrix},$$

kde $\mathbb{E}_k$ 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[45]. 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[46] $u_1 = 100\cdots$, $u_2 = 010\cdots$, $u_3 = 001\cdots$. 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 4.14 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[47] 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

$$G_K = \begin{pmatrix} \mathbb{E}_k & \mathbb{A} \end{pmatrix},$$

pro nějakou matici $\mathbb{A}$. Hledanou bijekci mezi $\varphi : \mathbb{Z}_p^k \to K$ lze volit (podobně, jako v důkazu Věty 4.17) následovně: pro každé $u = u_1 u_2 \cdots u_k \in \mathbb{Z}_p^k$ položíme

$$\varphi(u) = \left((u_1\ u_2\ \cdots\ u_k) \cdot \begin{pmatrix} \mathbb{E}_k & \mathbb{A} \end{pmatrix} \right)^T = uv[48],$$

kde slovo v je vektor daný součinem

$$\left((u_1\ u_2\ \cdots\ u_k) \cdot \mathbb{A} \right)^T.$$

[45] To je ostatně vhodné vždy!

[46] Tři tečky ... naznačují, že nás hodnota čtvrtého až $n$tého znaku kódových slov u_1, u_2 a u_3 nezajímají.

[47] Nebo snad lze jeden z těchto vektorů napsat jako lineární kombinací ostatních? Umíte to se standardní bází?

[48] 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 4.22. *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 má znak různý od nuly a na zbylých místech je $u - v$ 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[49], dokázali jsme vlastně následující:

Pozorování 4.23. *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 4.24 (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.

[49] Fakt! V každém podprostoru je nulový vektor!

Existuje ještě jeden způsob, jak zjistit minimální vzdálenost lineárního kódu: s využitím kontrolní matice a inspekcí jejích sloupců. Vezměme si kód z předchozího 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 4.25. *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[50] 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 této matice s koeficienty v_ℓ.

[50] Skutečně, z definice platí „K opravuje t-chyby $\Leftrightarrow \mu(K) > 2t \Leftrightarrow K$ objevuje $2t$-chyby“.

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 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

$$v \in K \;\Leftrightarrow\; \theta = H_K \cdot (v_1 \cdots v_n)^T = \sum_{j=1}^{n} v_j (H_K)_{:j} = \sum_{l=1}^{d} \underbrace{v_{i_l}}_{\neq 0} (H_K)_{:i_l} .$$

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. □

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 kontrolní matice neobsahuje nulový sloupec a nějaký sloupec kontrolní matice je násobkem jiného.

4.4 Dekódování

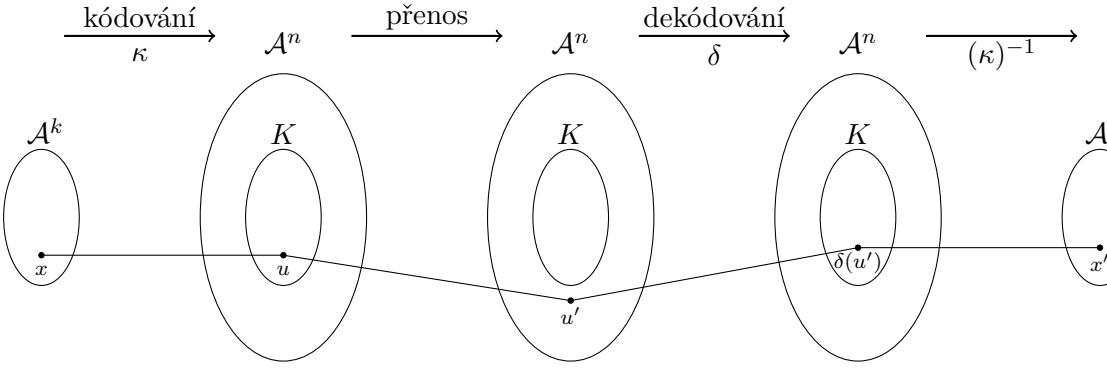
V první části jsme popisovali, jak zakódovat slovo. Pokud chceme poslat nějaké slovo $x \in \mathcal{A}^k$, tak jej nejdříve zakódujeme pomocí kódovací funkce κ na slovo $\kappa(x) = u \in K$, kde $K \subsetneq \mathcal{A}^n$ je lineární (n, k)-kód. Následně slovo u pošleme a přijmeme slovo u', které se kvůli šumu může lišit od u o chybu ε (tj. $u' = u + \varepsilon$).

Dekódování pro nás bude takové zobrazení δ, které slovu u' přiřadí nějaké kódové slovo (ideálně odeslané kódové slovo u). Potom již při troše štěstí[51] použitím inverzního zobrazení κ^{-1} obdržíme původní odeslané slovo $x = \kappa^{-1}(\delta(u'))$.

Definice 4.26. *Buď K lineární kód.* ***Dekódování***[52] *je libovolné zobrazení $\delta : \mathcal{A}^n \to K$ takové, že pro každé kódové slovo $\alpha \in K$ platí $\delta(\alpha) = \alpha$.*

[51] Tj. pokud chyb nebylo přespříliš.

[52] Povšimněme si, že dekódování není inverzní zobrazení ke kódování.



Obrázek 4.1: Schéma přenosu.

Pozorování 4.27. *Pokud lineární kód K opravuje t-chyby a definujeme*

$$\delta(u') := \text{„nejbližší kódové slovo k } u'\text{“},$$

potom pro každé kódové slovo $\alpha \in K$ a libovolnou chybu $\varepsilon \in \mathcal{A}^n$ takovou, že $\|\varepsilon\| \leq t$ platí

$$\delta(\alpha + \varepsilon) = \alpha.^{53}$$

Poznamenejme, že nejbližší kódové slovo k u' nemusí být právě jedno, potom z nabízených možností, můžeme zvolit libovolné jedno kódové slovo. V tomto případě existuje takových dekódovacích funkcí δ více.

Postup jak získat dekódovací funkci si demonstrujeme v následujícím příkladě.

Příklad 4.28. *Mějme lineární $(5, 2)$-kód K s generující maticí*

$$G_K = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Kód tedy obsahuje čtyři kódová slova: 00000,01101,11010,10111, z čehož přímo vidíme, že $\mu(K) = 3$. Tedy kód K objevuje 2 chyby a opravuje 1 chybu.

- *Buď $u' = 11100$. Hledáme $u \in K$ tak, že $d(u, u')$ je nejmenší.*
- *Najdeme $u = 11010$, chyba $u' - u = 00110$ a vzdálenost $d(u, u') = 2$, „nejmenší chybě“ 00110 budeme říkat **pivot slova** u' a značit $\pi_{u'}$.*
- *Všimněme si, že slova $00110 = 00000 + 00110, 01011 = 01101 + 00110, 10111 + 00110 = 10001$ mají stejný pivot.*

[53] Jinými slovy: opravuje-li kód t-chyby, potom uděláme-li v kódovém slově α ne více než t chyb, bude α nejbližší kódové slovo.

Najdeme-li ke každému slovu ze $\mathbb{Z}_2^5$ nejbližší kódové slovo (je-li jich více, vyberu si) a pivot, můžeme je zapsat do tabulky, kde první řádek jsou kódová slova, první sloupec pivoty. Slovo u' takové, že $u' = u + \pi_{u'}, u \in K$, zapíšeme do sloupce pod u a do řádku vedle $\pi_{u'}$, čímž získáme následující tabulku pro dekódování.

	pivot			
K:	00000	01101	11010	10111
	00001	01100	11011	10110
	00010	01111	11000	10101
	00100	01001	11110	10011
	01000	00101	10010	11111
	10000	11101	01010	00111
	00110	01011	11100	10001
	00011	01110	11001	10100

Jak postupovat v obecném případě si naznačíme v nadcházející definici, ale nejdříve si uvedeme pár pozorování.

Mějme K lineární (n, k)-kód, uvažujme variety W se zaměřením K (tj. $W = x + K$ pro nějaké $x \in \mathcal{A}^n$). Potom obdržíme:

1. Mějme W_1, W_2 variety se zaměřením K. Je-li $W_1 \cap W_2 \neq \emptyset$, potom $W_1 = W_2$.[54]
2. Jelikož $\#K = (\#\mathcal{A})^k$, každá varieta $W = x + K$ obsahuje právě $(\#\mathcal{A})^k$ prvků.

První bod nám, říká, že dvě různé variety se zaměřením K jsou disjunktní. Uvažujme všechny variety se zaměřením K. Každý prvek $z \in \mathcal{A}^n$ náleží nějaké varietě[55], obdržíme, že tyto variety, očíslujme si je $W_1, W_2, \ldots W_m$, pokrývají celý prostor $\mathcal{A}^n$. Průniky těchto variet jsou prázdné, a proto

$$\#\mathcal{A}^n = \#\left(\bigcup_{i=1}^{m} W_i\right) = \sum_{i=1}^{m} \#W_i.$$

Tedy

$$(\#\mathcal{A})^n = \#\mathcal{A}^n = \sum_{i=1}^{m} (\#\mathcal{A})^k = m \cdot (\#\mathcal{A})^k,$$

a proto nutně platí $m = (\#\mathcal{A})^{n-k}$.

Shrňme si to celé dohromady:

Pozorování 4.29. *Je-li K lin. (n, k)-kód nad abecedou $\mathcal{A}^n$ velikosti q, potom existují variety $W_i \in \mathcal{A}^n$ se zaměřením K, kde $i \in \{1, \ldots, q^{n-k}\}$, takové, že*

$$\mathcal{A}^n = \bigcup_i W_i \quad a \quad W_i \cap W_j = \emptyset, \text{ pro } i \neq j.$$

[54] Z Věty 3.41: Existuje-li z v průniku, tak potom $W_1 = z + K = W_2$.

[55] Třeba $z + K$.

Jinými slovy, prostor $\mathcal{A}^n$ lze rozložit na disjunktní variety se zaměřením K. Takových variet je $(\#\mathcal{A})^{n-k}$.

Pro ty z vás, co již znají pojem ekvivalence[56], se dá přepsat předchozí pozorování i jinými slovy:

Poznámka 4.30. *Je-li K lineární (n,k)-kód, potom relace $\equiv_K$ definovaná na $\mathcal{A}^n$ předpisem*

$$\xi \equiv_K \eta \iff \xi - \eta \in K$$

je ekvivalence.

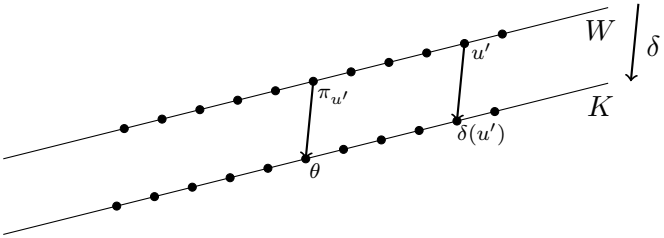
Prostor $\mathcal{A}^n$ se pak rozkládá na třídy ekvivalence

$$K + \xi = \{\kappa + \xi \mid \kappa \in K\}.^{57}$$

Každá třída obsahuje $\#K = q^k$ slov, kde $q = \#\mathcal{A}$. Počet všech tříd je q^{n-k}.

Definice 4.31. *Buď K lineární (n,k)-kód. V každé varietě W se zaměřením K[58] zvolíme slovo nejmenší Hammingovy váhy, tzv. **pivot**[59]. Definujeme $\pi_{u'}$ jako pivot třídy, ve které leží u'. Potom definujeme **standardní dekódování** δ vztahem:*

$$\delta(u') := u' - \pi_{u'}.^{60} \tag{4.3}$$



Obrázek 4.2: Schéma dekodování pro prvky variety $W = x + K$.

Pro lineární kód K si můžeme vytvořit **tabulku pro standardní dekódování**:

[56] Mimo jiné studenti s BI-ZDM.

[57] Každá třída odpovídá právě jedné varietě se zaměřením K.

[58] Neboli: každé třídě ekvivalence $\equiv_K$.

[59] Takových slov může být obecně více, zvolíme jedno takové. Volbou pivotu určíme, které slovo z W se dekóduje na θ. Pro ostatní slova variety se dekódování dopočítá pomocí předpisu (4.3).

[60] Rozmyslete si, že jsou-li $x, y \in W$, potom z Věty 3.41 máme $x + Z(W) = y + Z(W)$ a taky $x - y \in Z(W) = K$. Tedy vskutku $\delta(u') \in K$.

	pivot						
K:	θ	α_2	α_3	$\dots$	α	$\dots$	α_p
	β_1	β_2	β_3	$\dots$		$\dots$	β_p
	γ_1	γ_2	γ_3	$\dots$		$\dots$	γ_p
	$\vdots$	$\vdots$	$\vdots$				$\vdots$
	σ			$\dots$	τ	$\dots$	
	$\vdots$	$\vdots$	$\vdots$				$\vdots$

Povšimněme si

- V prvním sloupci jsou pivoty, všechny pivoty se dekódují na θ.
- V řádcích jsou vypsány všechna slova z variety $\sigma + K$ pro pivoty σ.
- $\beta_i = \alpha_i + \beta_1$, $\gamma_i = \alpha_i + \gamma_1$,
- přijaté τ najdeme v tabulce a dekódujeme jako slovo α nacházející se ve stejném sloupci v prvním řádku,
- $\delta(\tau) = \alpha = \tau - \sigma = \tau - \pi_\tau$,
- tabulka má $p = q^k$ sloupců a q^{n-k} řádků, kde $q = \#\mathcal{A}$.

Tato tabulka je s rostoucí velikostí kódu velmi velká a vyhledávání v ní zabere netriviální množství času. Ukážeme si, jak snížit náročnost dekódování.

Definice 4.32. *Buď K lineární kód.* ***Syndromem*** *slova $u' \in \mathcal{A}^n$ nazýváme slovo $\sigma_{u'} := H_K \cdot u'$.*

Pozorování 4.33.

- *$\sigma_{u'} = \theta$ právě pro $u' \in K$*
- *$\sigma_{u'} = \sigma_{v'}$ právě tehdy, když $u' + K = v' + K$*[61]*.*
- *Je-li $u \in K$ a $u' = u + \varepsilon$, pak $\sigma_{u'} = \sigma_\varepsilon$. Tedy syndrom přijatého slova u' splývá se syndromem příslušného chybového slova ε.*

Syndromová tabulka pro standardní dekódování:

pivot	$\varepsilon_1 = \theta$	ε_2	$\dots$	ε_r
syndrom	$\sigma_1 = \theta$	σ_2	$\dots$	σ_r

Dekodér přijme u', spočítá syndrom $\sigma_{u'}$, najde $i \in \hat{r}$ tak, že $\sigma_i = \sigma_{u'}$ a dekóduje

$$\delta(u') = u' - \varepsilon_i.$$

[61] což platí právě, když $u' \equiv_K v'$

Příklad 4.34. *Uvažujme ještě jednou předchozí příklad s binárním lineárním* $(5,2)$*-kódem* K *definovaným generující maticí*

$$G_K = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Spočítáme

$$H_K = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Syndromová tabulka:

pivot	*00000*	*00001*	*00010*	*00100*	*01000*	*10000*	*00110*	*00011*
syndrom	*000*	*110*	*011*	*100*	*010*	*001*	*111*	*101*

Přijme-li dekodér např. slovo $u' = 11111$*, spočítá* $\sigma_{u'} = H_K \cdot 11111 = 010$*. V pátém sloupci syndromové tabulky najde* $\varepsilon = 01000$ *a dekóduje:*

$$\delta(11111) = 11111 - 01000 = 10111.$$

4.5 Dodatky

Tato sekce je věnována studentům, kteří mají zájem lehce hlouběji nakouknout do tématu kódování. Stejně jako u dodatků v ostatních kapitolách nebudou znalosti zde obsažené vyžadovány u zkouškových či zápočtových písemek.

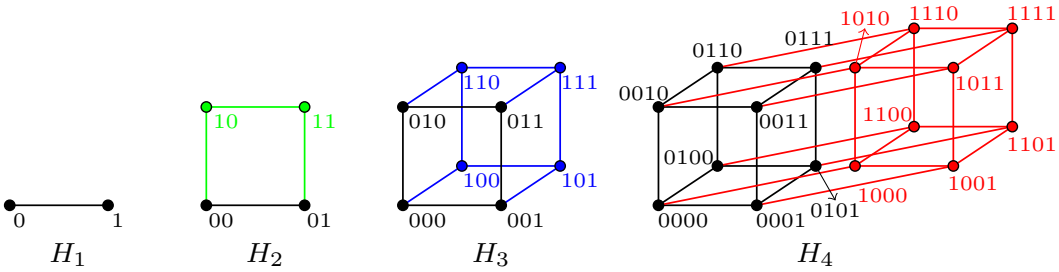
Hyperkrychle

V minulé sekci, jsme si zabývali lineárními kódy nad konečnou abecedou. Jistě nebude překvapením, že pro přímou aplikaci v IT jsou nejdůležitější kódy nad abecedou $\mathbb{Z}_2$. Tyto kódy se nazývají **binární kódy**. Ukážeme si, jak si tyto kódy vizualizovat pomocí **hyperkrychlí**.[62]

Konstrukce 4.35. *Hyperkrychle* H_1 *bude úsečka* $\langle 0,1\rangle$ *s vrcholy* 0 *a* 1*. Hyperkrychli* H_n *vytvoříme pomocí* H_{n-1} *takto:*

1. *Vytvoříme si dvě kopie* H_{n-1}*, označme si je* H^0_{n-1} *a* H^1_{n-1}*.*
2. *Vrcholům v* H^0_{n-1} *přidáme prefix* 0[63] *a těm v* H^1_{n-1} *prefix* 1*.*
3. *Spojíme úsečkou vrcholy v* H^0_{n-1} *se svou odpovídající kopií v* H^1_{n-1}*.*[64]

[62] Pozor, neplést s apakrychlemi!
[63] Neboli přidáme před označení znak 0, např $1011 \to \mathbf{0}1011$.
[64] Tedy spojíme každý vrchol tvaru $0u$ s vrcholem ve tvaru $1u$.



Vášnivý čtenář si pomocí matematické indukce snadno dokáže následující pozorování

Pozorování 4.36. *1. Hyperkrychle H_n má 2^n vrcholů.*

2. *Každý vrchol $v \in H_n$ má unikátní označení délky n složené z 0 a 1, neboli každému vrcholu odpovídá právě jedno slovo ze $\mathbb{Z}_2^n$.*

3. *Každý vrchol z H_n je spojen právě s n vrcholy H_n.*

4. *Vrcholy $u, v \in H_n$ jsou spojeny, právě když se liší jejich označení v jednom znaku.*[65]

5. *Minimální počet hran, které musíme projít, abychom se z vrcholu $u \in H_n$ dostali do vrcholu $v \in H_n$ je $d(u, v)$.*

Binární Hammingovy kódy

V této části si popíšeme jedny poměrně jednoduché, ale přesto velmi užitečné kódy, a to binární Hammingovy kódy. Richard Hamming byl americký matematik, jehož dílo mělo nesmírný dopad zejména v telekomunikaci a počítačovém inženýrství. V dobách, kdy se programy ukládaly na děrné štítky, docházelo často k chybám. Počítač byl sice schopen detekovat, že k nějaké chybě došlo, ale bohužel ji nebyl schopen najít natož opravit. Tímto byl Richard Hamming motivován ke studiu samoopravných kódů. Hammingovy kódy detekují dvoj-chyby a opravují jednu chybu, a tak se používají v oblastech, kde je pravděpodobnost chyby nízká, například v ECC[66] pamětích, či při zapojení disků do Raid 2.

Definice 4.37. *Buď $m \geq 2$. Lineární $(2^m - 1, 2^m - 1 - m)$ kód K s kontrolní maticí H_K, v jejímž i-tém sloupci jsou zapsány cifry čísla $i \in \{1, 2, \ldots, 2^m - 1\}$ ve dvojkové soustavě (na m pozicích), nazýváme **binární Hammingův kód**.*

Nejdříve si ukážeme, jak kód vypadá pro některé konrétní m.

[65] Tj. právě když $d(u, v) = 1$.
[66] Error-correcting code.

Příklad 4.38. *1. Je-li $m = 2$, potom máme $(3,1)$-kód, a kontrolní matice je ve tvaru:*

$$H_K = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

Snadno dopočítáme, že Hammingův $(3,1)$-kód obsahuje pouze dvě kódová slova 000 a 111, neboli v tomto případě splývá s již známým 3-opakovacím kódem.

2. Pro $m = 3$, obdržíme $(7,4)$-kód s kontrolní maticí

$$H_K = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Lehce spočítáme generující matici

$$G_K = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Tento binární kód je tedy generován pomocí čtyř slov, proto má celkem šestnáct slov.

$$K = \{0000000, 1000011, 0100101, 0010110, 0001111, 1100110, 1010101, 1001100,$$
$$0110011, 0101010, 0011001, 0111100, 1011010, 1101001, 1110000, 1111111\}$$

Věta 4.39. *Pro binární Hammingův kód K platí $\mu(K) = 3$. Tedy K objevuje 2-chyby a opravuje 1-chyby.*

Důkaz. Sloupce kontrolní matice H_K neobsahují nulový sloupec a jsou navzájem různé. Proto z Věty 4.25 plyne $\mu(K) > 2$.

Na druhou stranu v matici H_K lze vždy najít 3 sloupce, které tvoří LZ soubor (např. první tři sloupce, které jsou dvojkovým zápisem čísel 1 a 2 a jejich součet 3). Proto je $\mu(K) \leq 3$. Celkem tedy obdržíme $\mu(K) = 3$. □

Binární Hammingův kód máme již dobře nastudován, proto již může přikročit k jeho dekódování.

Věta 4.40. *Buď K binární $(2^m - 1, 2^m - 1 - m)$ Hammingův kód. Množina pivotů všech variet se zaměřením K[67] je tvořena vektory standardní báze ε_i prostoru $\mathbb{Z}_2^n$ (kde $n = 2^m - 1$) a nulovým vektorem θ.*

[67] neboli tříd ekvivalence $\equiv_K$.

Důkaz. Z Pozorování 4.29 se celý prostor rozkládá na 2^{n-k} variet se zaměřením K. Protože $n = 2^m - 1$ a $k = 2^m - 1 - m$, máme, že těchto variet je $2^{n-k} = 2^m$.

Slovo θ je pivotem třídy K. Jelikož pro každé $i \in \hat{n}$ je $\|\varepsilon_i\| = 1$, tvrzení věty bude pravdivé, pokud pro každé $i, j \in \hat{n}, i \neq j$ jsou ε_i a ε_j prvky různých dvou variet se zaměřením K.

To poznáme tak, že syndromy $\sigma_i := H_K \cdot \varepsilon_i$ a $\sigma_j := H_K \cdot \varepsilon_i$ budou různé.

Nyní si stačí uvědomit, že díky vlastnostem maticového násobení je slovo $H_K \cdot \varepsilon_i$ právě i-tý sloupec matice H_K. Tedy σ_i je i-tý sloupec H_K. Protože libovolné dva sloupce H_K jsou různé, dostáváme, že $\sigma_i \neq \sigma_j$. □

Protože $\sigma_i = H_K \cdot \varepsilon_i = h_i$, kde h_i je i-tý sloupec H_K, což je právě číslo i zapsané v dvojkové soustavě, má syndromová tabulka pro standardní dekódování K tvar:

pivot	θ	ε_1	ε_2	$\ldots$	ε_n
syndrom	θ	h_1	h_2	$\ldots$	h_n

Tedy dekodér přijme slovo β, přečte σ_β jako dvojkový zápis čísla i a opraví i-tý znak v β.

Příklad 4.41. *Hammingův kód pro $m = 4$ je $(15, 11)$-kód s kontrolní maticí*

$$H_K = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Dekodér přijme např. slovo $\beta = 001001000000001$. Potom $\sigma_\beta = 1010$ a protože $(1010)_2 = 10$, opraví 10. znak ve slově β:

$$\delta(001001000000001) = 001001000\mathbf{1}00001.$$

Lineární kódy a pravděpodobnost

V této části si popíšeme, jak spočítat, o kolik naše lineární kódy zvyšují šanci na úspěšný přenos dat. Výpočet pravděpodobnosti nám ulehčí následující pozorování:

Pozorování 4.42. *Mějme kódové slovo $u \in K$, po přenosu obdržíme slovo $u + \varepsilon$, kde ε je případná chyba. Potom chybu nedetekujeme, právě když $u + \varepsilon \in K$. To je právě tehdy, když $\varepsilon \in K$.*

Věta 4.43. *Máme-li lineární kód $K \subset\subset \mathbb{Z}_2^n$ a je-li pravděpodobnost úspěšného přenosu bitu $p \in \langle 0, 1\rangle$, potom pravděpodobnost, že nastane chyba, která nebude detekovaná, je*

$$P = \sum_{u \in (K \setminus \{\theta\})} p^{n-\|u\|} \cdot (1-p)^{\|u\|}.$$

Důkaz. Díky předchozímu pozorování víme, že chybu ε při přenosu neodhalíme právě tehdy, když $\varepsilon \in K\backslash\{\theta\})$. Očíslujme si nenulová kódová slova $(K\backslash\{\theta\}) = \{u^1, u^2, \dots u^m\}$.

Jaká je pravděpodobnost, že nastane neidentifikovatelná chyba $\varepsilon^j = u^j \in \mathbb{Z}_2^n$? Pro vznik chyby ε^j by musela nastat chyba přesně na té pozici, kde je $(u^j)_i \neq 0$, což je právě na $\|u^j\|$ pozicích, a nevzniknout chyba, pokud $(u^j)_i = 0$, což je pro $n - \|u^j\|$ zbylých pozic.

Proto šance, že vznikne neidentifikovaná chyba $\varepsilon^j = u^j \in K$, je

$$P(\varepsilon^j) = \underbrace{p^{n-\|u^j\|}}_{n-\|u^j\| \text{ bitů se přenese správně.}} \cdot \underbrace{(1-p)^{\|u^j\|}}_{\text{V } \|u^j\| \text{ bitech nastane chyba.}}.$$

Celkově obdržíme

$$P = \sum_{j=1}^{m} P(\varepsilon^j) = \sum_{j=1}^{m} p^{n-\|u^k\|} \cdot (1-p)^{\|u^j\|} = \sum_{u \in (K\backslash\{\theta\})} p^{n-\|u\|} \cdot (1-p)^{\|u\|}.$$

□

Příklad 4.44. *Mějme přenosový kanál takový, že šance na úspěšný přenos jednoho bitu je* $p = 0,8$.[68] *Uvažujme* 3*-opakovací kód* $K \subseteq \mathbb{Z}_2^6$.[69] *Všechny kódová slova jsou*

$$K = \{000000, 010101, 101010, 111111\}.$$

Díky předchozí větě obdržíme, že pravděpodobnost vzniknutí nedetekované chyby je

$$\begin{aligned} P = (0,8)^{n-\|010101\|}(1-0,8)^{\|010101\|} &+(0,8)^{n-\|010101\|}(1-0,8)^{\|101010\|} \\ &+(0,8)^{n-\|111111\|}(1-0,8)^{\|111111\|} \\ = 2(0,8)^3(0,2)^3 + (0,2)^6 &= 0,008256. \end{aligned}$$

Tedy šance na nedetekování chyby je menší než 1%.

Pro ilustraci si uveďme následující tabulku pro přenos 4-bitové informace, za předpokladu, že šance na úspěšný přenos jednoho bitu je $p = 0,9$.

kód	kontr. bity	celkem bity	poměr infor./celkem	pr. úspěšného přenosu[70]	pr. nerozpoznání chyby[71]
bez kódování	0	4	1	0,6561	0,3439
paritní	1	5	0,8	0,5905	0,0734
3-opakovací	8	12	0,3333	0,2824	0,0016
5-opakovací	16	20	0,2	0,1216	$8 \cdot 10^{-6}$
Hammingův	3	7	0,5714	0,4782	0,0051
Hadamardův	12	16	0,25	0,1853	$6 \cdot 10^{-8}$
propíchnutý Hadamardův	4	8	0,5	0,4305	0,009

[68] neboli 80 %.

[69] Neboli slovu o dvou bitech u_1u_2 přiřadíme šestibitové slovo $u_1u_2u_1u_2u_1u_2$.

Jak se pravděpodobnost úspěšného přenosu změní, pokud využijeme standardní dekódování, které nám opraví některé chyby? Opět začneme pozorováním:

Pozorování 4.45. *Mějme kódové slovo $u \in K$, po přenosu obdržíme slovo $u+\varepsilon$, kde ε je případná chyba. Potom slovo $u+\varepsilon$ dekódujeme správně, právě když ε je pivot nějaké variety W se zaměřením K.*

Důkaz. Pomocí Definice 4.31 standardního dekódování obdržíme, že dekódování bude úspěšné, jen pokud platí rovnice

$$u = \delta(u+\varepsilon) = u + \varepsilon - \pi_{u+\varepsilon},$$

která platí pouze tehdy, když $\varepsilon = \pi_{u+\varepsilon}$. Což ale platí, právě když ε je pivot variety se zaměřením K. □

Předchozí pozorování můžeme přetlumočit do tvaru: Standardní dekódování opraví jen ty chyby, které jsou pivoty variet se zaměřením K. Z Pozorování 4.29 víme, že variet se zaměřením K je $(\#\mathcal{A})^{n-k}$. Tedy standardní dekódování opraví právě $(\#\mathcal{A})^{n-k}$ různých chyb.

Vyzbrojeni předchozím pozorováním se můžeme pustit do následující věty.

Věta 4.46. *Mějme lineární kód $K \subset\subset \mathbb{Z}_2^n$ a předpokládejme, že pravděpodobnost úspěšného přenosu jednoho bitu je $p \in \langle 0,1\rangle$. Označme si α_j jako počet těch pivotů takových, jejichž Hammingova váha je j.*[72] *Potom pravděpodobnost úspěšného dekódování je*

$$P = \sum_{j=0}^{n} \alpha_j \; p^{n-j} \cdot (1-p)^j.$$

Důkaz. Uvažujme všechny chyby s Hammingovou váhou j (tzn. chyba přenosu slova délky n nastala v j bitech). Šance, že nastane tato chyba, která změní právě j bitů, je

$$p^{n-j} \cdot (1-p)^j.$$

Nyní uvažujme jenom ty chyby Hammingovou váhy j, která jsme schopni opravit. Díky předchozímu pozorování víme, že to jsou právě ty chyby, jež jsou pivoty nějaké variety W se zaměřením K. Takových je pivotů je α_j. Proto pravděpodovnost P_j, že odhalíme změnu v j bitech, je

$$\alpha_j \cdot p^{n-j} \cdot (1-p)^j.$$

[70] Pravděpodobnost, že všechny bity byly obdrženy bez chyby.

[71] Pravděpodobnost, že zároveň nastala chyba a nebyla rozpoznána

[72] Neboli α_j je počet takových variet se zaměřením K takových, že obsahují slovo s j jedničkami a každé další slovo má alespoň j jedniček.

Celkově

$$P = \sum_{j=0}^{n} P_j = \sum_{j=0}^{n} \alpha_j \; p^{n-j} \cdot (1-p)^j.$$

□

Příklad 4.47. *Aplikujeme předchozí větu na 3-opakovací kód $K \subseteq \mathbb{Z}_2^6$ z Příkladu 4.44. Opět uvažujme přenosový kanál takový, že šance na úspěšný přenos jednoho bitu je $p = 0,8$.*

Kód má kontrolní matici

$$H_K = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Při vytváření syndromové tabulky najdeme všech $2^4 = 16$ pivotů:

pivot	*000000*	*100000*	*010000*	*001000*	*000100*	*000010*	*000001*	*110000*
syndrom	*0000*	*1010*	*0101*	*1000*	*0100*	*0010*	*0001*	*1111*
pivot	*100100*	*100001*	*011000*	*010010*	*001100*	*001001*	*000110*	*000011*
syndrom	*1110*	*1011*	*1101*	*0111*	*1100*	*1001*	*0110*	*0011*

Zjistili jsme, že máme 1 pivot Hammingovy váhy 0 (neboli $\alpha_0 = 1$), 8 pivotů váhy 1 ($\alpha_1 = 8$) a 7 pivotů váhy 2 ($\alpha_2 = 7$). Díky předchozí větě obdržíme, že pravděpodobnost úspěšného přenosu při standardním dekódování je

$$P = (0,8)^6 + 8 \cdot (0,8)^7(1-0,8)^1 + 7 \cdot (0,8)^6(1-0,8)^2 = 0,671089.$$

Tedy šance na úspěšný přenos je asi 67%.

Opět si pro ilustraci si uveďme následující tabulku pro přenos 4-bitové informace, za předpokladu, že šance na úspěšný přenos jednoho bitu je $p = 0,9$ při užití **pomocí standardního dekódování**.

kód	poměr infor./celkem	pr. úspěšného dekodování[73]	pr. chybného přenosu[74]
bez kódování	1	0,6561	0,3439
paritní	0,8	0,6561	0,3439
3-opakovací	0,3333	0,8926	0,1074
5-opakovací	0,2	0,9662	0,0337
Hammingův	0,5714	0,8503	0,1497
Hadamardův	0,25	0,9738	0,0152
propíchnutý Hadamardův	0,5	0,8503	0,1497

Možná si říkáte, proč se zlepšila šance na úspěšný přenos u paritního kódu oproti předešlé tabulce, když přece tento kód žádné chyby neopravuje? Rozmysleme si, co dělá standartní dekódování. Nejdříve si prostor rozdělí na dvě variety

$$\begin{aligned} W_1 = K = \{&00000, 11000, 10100, 10010, 10001, 01100, 01010, 01001,\\ &00110, 00101, 00011, 11110, 11101, 11011, 10111, 01111\}\\ W_2 = \{&10000, 01000, 00100, 00010, 00001, 00111, 01011, 01101,\\ &01110, 10011, 10101, 10110, 11001, 11010, 11100, 11111\}. \end{aligned}$$

Poté určí ve varietě W_2 pivot, např 00010 a každé slovo $u \in W_2$ dekóduje $d(u) = u - 00010$.[75] Tedy za předpokladu, že nastala jedna chyba máme stále šanci opravit zprávu dobře. A to právě v 20%, protože zprávu s jednou chybou opravíme správně pouze v případě, když chyba byla ve čtvrtém bitu. V 80% případů při jedné chybě zprávu přeložíme špatně.

MDS kódy

Ve Větě 4.15 jsme se dozvěděli, že minimální velikost lineárního (n, k)-kódu je seshora omezena $\mu(K) \leq n - k + 1$.. Pokud v této formuli dosáhneme rovnosti, obdržíme maximální možný poměr informační bity/kontrolní bity. Kódy s touto velmi užitečnou vlastností se nazývají **MDS** kódy[76]. Proto si o nich řekneme něco více.

Snadno si rozmyslíme, že triviální (a tedy neužitečné) (n, n) a $(n, 0)$-kódy jsou MDS. Příkladem užitečnějšího MDS kódu jsou paritní kód (který je typu $(n, n-1)$) a n-opakovací kód (který je typu $(n, 1)$).

Ukážeme si, že žádné jiné binární MDS kódy neexistují!

Věta 4.48. *Nechť $n \in \mathbb{N}$. Všechny binární lineární MDS kódy jsou pouze typu $(n, 0)$, $(n, 1)$, $(n, n-1)$, (n, n).*

Důkaz. Víme, že kódy vhodných typů existují, proto nám již stačí jen ukázat, že neexistují MDS kódy pro $2 \leq k \leq n-2$. Pro spor předpokládejme, že pro nějaké takové k existuje MDS kód K, tj. $\mu(K) = n - k + 1$.

Můžeme předpokládat, že kód je systematický (jinak bychom vyměnili pořadí bitů v kontrolní matici, tak aby byl), a tedy generující matice G_K je ve formě $(\mathbb{E}_k \; \mathbb{A})$, kde $\mathbb{E}_k \in \mathbb{Z}_2^{k,k}$ a $\mathbb{A} \in \mathbb{Z}_2^{k,n-k}$.

Řádky matice G_K mají v prvních k složkách právě jednu jedničku a $k-1$ nul. Tyto řádky G_K jsou kódová slova, jejichž váha musí být dle předpokladu o minimální

[73] Pravděpodobnost, že chyb při přenosu bylo málo, a zprávu jsme po případné opravě obdrželi.
[74] Pravděpodobnost, že jsme zprávu dekódovali špatně.
[75] Tedy změní čtvrtý bit.
[76] Z anglického maximum distance separable.

vzdálenosti kódu alespoň $n-k+1$ (neboli tato slova obsahují alespoň $n-k+1$ nenul), z čehož zřejmě vyplývá, že všechny prvky matice $\mathbb{A}$ jsou jedničky.

Jelikož je $k \geq 2$, generující matice obsahuje aspoň dva řádky. Protože kód je podprostor, je $(G_K)_{1:}+(G_K)_{2:}$ kódové slovo. Povšimněme si, že obsahuje právě dvě jedničky (v první a druhé souřadnici), tedy toto kódové slovo má váhu právě 2. Proto $\mu(K) \leq 2$.

Celkově obdržíme

$$n-k+1 = \mu(K) \leq 2 \;\Rightarrow\; n-1 \leq k$$

a to je spor s předpokladem $k \leq n-2$. □

Tedy pro hledání dalších MDS kódů musíme použít větší abecedu než $\mathbb{Z}_2$. Nejdůležitějším příkladem jsou **Reed–Solomonovy kódy**, které se mimo jiné používají v CD/ DVD přehrávačích při korekci chyb vzniklých poškozením disku, v QR kódech, v pozemním vysílání DVB-T, nebo při zapojení disků do Raid 6. Pro p prvočíslo a k přirozené číslo, Reed–Solomonův kód $RS_{p^k,k}$ je lineární (p^k-1,k)-kód nad abecedou $GF(p^k)$[77] s minimální vzdáleností $q-k$. Pro $k=1$ tento kód splývá s paritním kódem.

Další důležité kódy

Teorie kódování je stále živá, neustále se publikují nové a nové výsledky. Studium lineárních (nebo snad dokonce i nelineárních) kódu, by vydalo na mnohem rozsáhlejší text, než mají tato celá skripta BI-LIN dohromady. Proto si už jen krátce zmiňme některé další kódy

- **Golayovy kódy** jsou lineární kódy užívané v radiokomunikaci, například sondy Voyager 1 a 2 je užívaly při své cestě mimo solární systém k přenosu fotografií Jupiteru a Saturnu. Tyto kódy spolu s Hammingovými kódy, ℓ-opakovacími kódy pro ℓ liché a triviálními kódy $\{\theta\}$ a $\mathcal{A}^n$ tvoří jediné perfektní kódy.

- **Hadamardovy kódy**[78] jsou kódy užíváné k přenosu informací v hodně zarušeném prostředí. Proto byly užity u mise sondy Mariner 9 k přenosu fotografií Marsu zpátky na Zem. Jsou optimální ve své třídě.[79]

- **Turbo-kódy** jsou vysoce výkonné[80] neblokové kódy (tedy nespadají mezi naše lineární kódy), používané v telekomunikacích. Je na nich založena technologie 3G/4G, či komunikace se satelity a sondami ve vesmíru. Patři mezi konvoluční kódy.

[77] $GF(p^k)$ je těleso velikosti p^k, viz část Dodatek ke konečným tělesům 1.7.

[78] Také známe jako Walshovy kódy.

[79] Neboli neexistuje žádný binární kód, který by opravoval stejně chyb ale potřeboval k přenosu méně znaků.

[80] tj. mají výborný poměr „informační/ kontrolní“ bity.

- **LDPC kódy**[81] jsou lineární kódy, jejichž kvalita je srovnatelná s Turbo-kódy. Z názvu vyplývá, že kontrolní matice tohoto kódu je velmi řídká (tzn., obsahuje velmi málo jedniček, skoro samé nuly). Jejich síla vyniká při velkých přenosových rychlostech, například u DVB-S2 (satelitní přenos digitálního signálu), 10GBase-T Ethernet, Wi-Fi 802.11n, Wi-Fi 802.11ac.

[81] LDPC = Low-density parity-check code, někdy také označované jako Gallagerovy kódy.

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 libovolných 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 lineárnímu 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.

[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.

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*.

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 **právě 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 právě jeden obraz, ale každý prvek z Y může mít libovolný počet vzorů při zobrazení f.

- **Obrazem množiny** $M \subseteq X$ rozumíme množinu

  $$f(M) = \{f(a) \in Y \mid a \in M\},$$

  podobně **vzor množiny** $N \subseteq Y$ značíme

  $$f^{-1}(N) = \{a \in X \mid f(a) \in N\}.$$

  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].
- 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 $g \circ f = id_X$.

5.3 Linearita a její důsledky

Definice 5.1. *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): $\forall \alpha \in T, \forall x \in P : A(\alpha x) = \alpha Ax$.*[7]

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.*

Definice 5.2. *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.*

[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).

[7] 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.

Izomorfismem *nazveme jakékoli zobrazení* $A \in \mathcal{L}(P,Q)$*, které je současně bijekce*[8].

Jak je patrno z předchozích definic, budeme u lineárních zobrazení používat značení mírně odlišné od například matematické analýzy. Rozdíly shrňme v poznámce.

Poznámka 5.3. *Oproti malým písmenům* $f, g, \dots$ *budeme pro lineární zobrazení mezi vektorovými prostory používat písmena velká,* $A, B, \dots$*. 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!*

Pro ilustraci si uveďme několik jednoduchých příkladů lineárních zobrazení ve známých vektorových prostorech. Jejich linearitu si laskavý čtenář jistě pln nadšení ověří sám.

- $A : \mathbb{R} \to \mathbb{R}$,
$$Ax := \alpha x \text{ pro dané } \alpha \in \mathbb{R}\,,$$
- $B : \mathbb{C}^3 \to \mathbb{C}^2$,
$$B(x,y,z) := (x + 2y - z, x - 2y - 3z)\,,$$
- $C : T^\infty \to T^3$,
$$C(x_1, x_2, x_3, \dots) := (x_1, x_2, x_3)\,,$$
- $D : T^\infty \to T^\infty$,
$$D(x_1, x_2, x_3, \dots) := (x_2, x_3, x_4, \dots)\,,$$
- $E : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$,
$$E(x_1, x_2, \dots, x_{n-1}, x_n) := (x_2, x_3, \dots, x_n, x_1)\,,$$
- $F : \mathbb{R}^\infty \to \mathbb{R}^\infty$,
$$F(x_1, x_2, x_3, \dots) := (x_2 - x_1, x_3 - x_2, x_4 - x_3, \dots)\,,$$

[8] 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.

- $G : \mathbb{R}^{2,2} \to \mathbb{R}^{2,2}$,
$$G\begin{pmatrix} a & b \\ c & d \end{pmatrix} := \begin{pmatrix} a+b & a-b \\ c-d & c+d \end{pmatrix},$$

- Ve vektorovém prostoru $\mathcal{P}$ všech polynomů s operacemi sčítání polynomů a násobení polynomu číslem[9] je operace derivování lineárním zobrazením, tj. $H : \mathcal{P} \to \mathcal{P}$,
$$Hp = p',$$

Ovšem například zobrazení $I : \mathbb{R} \to \mathbb{R}$ definované předpisem $Ix = x + 1$ dle Definice 5.1 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.

Již v kapitole Základní pojmy lineární algebry jsme se s jedním lineárním zobrazením setkali, aniž bychom to vlastně věděli. A to se souřadnicovým funkcionálem, resp. s přiřazením $n$tice souřadnic vůči zadané bázi.

Věta 5.5. *Nechť* $\mathcal{X}$ *je báze prostoru* V_n *nad* T*. Přiřazení* $(\cdot)_\mathcal{X} : V_n \to T^n$ *definované předpisem* $z \mapsto (z)_\mathcal{X}$ *je lineární zobrazení, kde* $(z)_\mathcal{X}$ *značí souřadnice vektoru* z *vůči bázi* $\mathcal{X}$ *jako v Definici 2.71. Navíc se jedná o bijekci, tedy je to izomorfismus (tzv.* ***souřadnicový izomorfimus****).*

Souřadnicový funkcionál $x_i^\# : V_n \to T$ *je lineární funkcionál.*

Důkaz. Nechť $x, y \in V_n$, označme jejich souřadnice v bázi $\mathcal{X}$ následovně:
$$x = \sum_{i=1}^{n} \alpha_i x_i, \qquad y = \sum_{i=1}^{n} \beta_i x_i.$$
Odtud rovnou plyne
$$x + y = \sum_{i=1}^{n} \alpha_i x_i + \sum_{i=1}^{n} \beta_i x_i = \sum_{i=1}^{n} (\alpha_i + \beta_i)\, x_i.$$

[9] Opravdu se jedná o vektorový prostor. Kdo nevěří, nechť si to dokáže.
[10] Ačkoli v kontextu matematické analýzy bychom ho nazvali lineární funkcí.

Protože souřadnice vektoru v dané bázi jsou určeny jednoznačně, získáváme

$$(x+y)_{\mathcal{X}} = (\alpha_1+\beta_1, \ldots, \alpha_n+\beta_n) = (x)_{\mathcal{X}} + (y)_{\mathcal{X}}$$

a stejně tak pro každé $i \in \hat{n}$ platí

$$x_i^{\#}(x+y) = \alpha_i + \beta_i = x_i^{\#}(x) + x_i^{\#}(y)\,.$$

Vlastnosti $(\alpha x)_{\mathcal{X}} = \alpha(x)_{\mathcal{X}}$ a $x_i^{\#}(\alpha x) = \alpha x_i^{\#}(x)$ si pozorný čtenář snadno dokáže analogicky.

Zbývá si jen rozmyslet, že $(\cdot)_{\mathcal{X}}$ je bijekce. Je-li $(x)_{\mathcal{X}} = (y)_{\mathcal{X}}$, potom

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

a tedy $x = y$. Proto je toto zobrazení injektivní.

Máme-li libovolnou $n$tici $(\alpha_1, \ldots, \alpha_n) \in T^n$ pak pro

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

je zřejmě $(x)_{\mathcal{X}} = (\alpha_1, \ldots, \alpha_n)$. Tedy zobrazení je i surjektivní. □

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 5.6. *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) $\forall n \in \mathbb{N}, \forall \alpha_1, \ldots, \alpha_n \in T, \forall x_1, \ldots, x_n \in P :$

$$A\left(\sum_{i=1}^{n} \alpha_i x_i\right) = \sum_{i=1}^{n} \alpha_i A x_i.$$ [11]

[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.

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 3.20. Konkrétně při důkazu implikace $(ii) \Rightarrow (iii)$ je pak vhodné použít matematickou indukci podle n.

Laskavý čtenář pak může (náležitě rozcvičen právě provedeným důkazem) rovnou pokračovat důkazem dalšího pozorování, a to o linearitě inverzních a složených zobrazení.

Pozorování 5.7.

(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 5.8. *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

$$A\theta_P = \theta_Q\,.$$

(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 $\mathcal{X} = (x_1, \ldots, x_n)$ v P a $\mathcal{Y} = (y_1, \ldots, y_n)$ 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 „předobraz“[14] $\mathcal{X}$ je LN.

[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 5.6) skutečně nic víc nepotřebujeme.

[14] Pro každý vektor z $\mathcal{Y}$ je v $\mathcal{X}$ pouze jeden vybraný vzor (tj. $x_i \in A^{-1}(y_i)$).

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 $\alpha_1, \ldots, \alpha_n \in T$ a $x_1, \ldots, x_n \in M$ 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 $Ax_1, \ldots Ax_n$, 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 $(x_1, \ldots, x_n)$ je LZ soubor v P. Existují tedy koeficienty $\alpha_1, \ldots, \alpha_n \in T$, 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.

□

Jak vyplývá z příkladů uvedených výše, lineární zobrazení mezi VP lze jistě definovat zadáním explicitního vzorečku[15]. 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[16] a tím je už hledané zobrazení $A \in \mathcal{L}(P, Q)$ jednoznačně určeno!

Věta 5.9. *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,

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

Jelikož hledáme zobrazení A splňující $Ax_i = y_i$ pro každé $i \in \hat{n}$, které je současně lineární, nutně musí dále platit:

$$A\left(\sum_{i=1}^{n} \alpha_i x_i\right) = \sum_{i=1}^{n} \alpha_i A x_i = \sum_{i=1}^{n} \alpha_i y_i \,.$$

Tedy hledané zobrazení předepíšeme pomocí souřadnic v bázi $(x_1, \ldots, x_n)$ pravidlem

$$z = \sum_{i=1}^{n} \alpha_i x_i \quad \Rightarrow \quad Az := \sum_{i=1}^{n} \alpha_i y_i \,.$$

Je ovšem třeba zdůvodnit, že takto definované zobrazení $A : P \to Q$ je skutečně 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 přiřazení souřadnic, viz Věta 5.5.

[15] Máme na mysli funkční předpis ve tvaru: „pro libovolné $x \in P$ platí $Ax = \ldots$ “.

[16] U kterého budeme tiše předpokládat konečnou dimenzi – v zájmu obecného blaha a jednoduššího důkazu.

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 $b \in P$ takový, že $Bb \neq Ab$. Označme $(b)_{\mathcal{X}} = (\beta_1, \beta_2, \ldots, \beta_n)$, z linearity B pak dostáváme

$$Bb = B\left(\sum_{i=1}^{n} \beta_i x_i\right) = \sum_{i=1}^{n} \beta_i B x_i = \sum_{i=1}^{n} \beta_i y_i = Ab\,,$$

což je spor. □

Příklad 5.10. *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 5.11. *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

$$(z)_{\mathcal{X}} = (\alpha, \beta, \gamma) = (a-b, b-c, c)\,.$$

Pak už podobně jako v předchozím příkladu odvodíme

$$\begin{aligned} Bz &= B((a-b)x_1 + (b-c)x_2 + cx_3) \\ &= (a-b)Bx_1 + (b-c)Bx_2 + cBx_3 \\ &= (a-b)(1,1,1,1) + (b-c)(0,1,0,-1) + c(0,0,1,-1) \\ B(a,b,c) &= (a-b, a-c, a-b+c, a-2b)\,. \end{aligned}$$

[17] $e_1 = (1,0,0), e_2 = (0,1,0), e_3 = (0,0,1)$.

Poznámka 5.12. *Přijdou vám postupy v Příkladech 5.10 a 5.11 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...*

5.4 Hodnost, jádro a defekt zobrazení

Definice 5.13. *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 5.8 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!

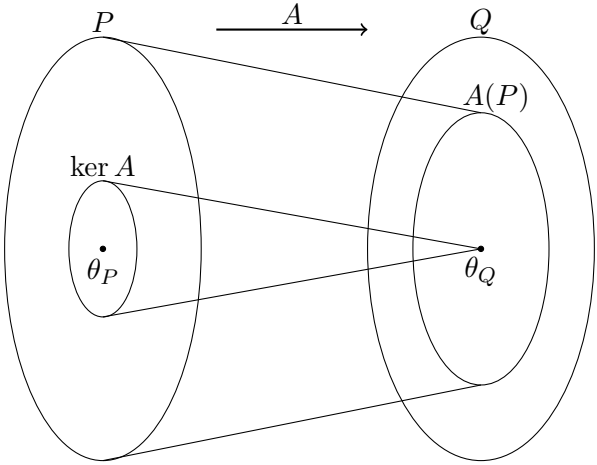
Příklad 5.14. *Odvodíme jádra lineárních zobrazení uvedených na začátku kapitoly. Ve všech případech je třeba vyřešit rovnici $Ax = \theta$, kde za x dosadíme obecný vektor v daném prostoru a za θ příslušný nulový vektor. To vždy povede na nějakou soustavu lineárních rovnic*[20]*, kterou snadno vyřešíme. Pro první tři příklady zobrazení uveďme celý postup řešení:*

- $A : \mathbb{R} \to \mathbb{R}$, $Ax := \alpha x$ 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

$$\ker A = \begin{cases} \{0\} = \{\theta_{\mathbb{R}}\} & \text{pro } \alpha \neq 0\,, \\ \mathbb{R} & \text{pro } \alpha = 0\,. \end{cases}$$

[18] Jde o vzor jednoprvkové množiny $\{\theta_Q\}$, která je triviálním podprostorem.
[19] Až téměř intimní.
[20] Jak překvapivé!



Obrázek 5.1: Ilustrace jádra a oboru hodnot pro $A \in \mathcal{L}(P, Q)$.

- $B : \mathbb{C}^3 \to \mathbb{C}^2$, $B(x, y, z) := (x + 2y - z, x - 2y - 3z)$:
  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* $\mathcal{X} = (x_1, \ldots, x_n)$.

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, který 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 $x = y$. □

Ve Větě 5.8 jsme si mimo jiné 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.

Věta 5.16. *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.*

[21] Tedy ověření, zda $Ax = Ay$ implikuje $x = y$.

Důkaz. (i) Je-li $(y_1, \dots, y_n)$ LZ soubor vektorů z Q, existují $\alpha_1, \dots, \alpha_n \in T$ 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 $(x_1, \dots, x_n)$ je LZ.

(ii) Kdyby existoval LN soubor, jehož obraz by byl LZ, dostali bychom se do sporu s bodem (i).

□

Právě dokázáná věta nám společně s Větou 5.8 (iv) dává následující důsledek.

Důsledek 5.17. *Nechť $A \in \mathcal{L}(P, Q)$ je prosté. Pokud soubory $(x_1, \dots, x_n)$ v P a $(y_1, \dots, y_n)$ v Q splňují $Ax_i = y_i$ pro každé $i \in \hat{n}$, pak platí*

$$(x_1, \dots, x_n) \text{ je LN} \Leftrightarrow (y_1, \dots, y_n) \text{ je LN}.$$

Pro lepší pochopení pojmů hodnost a defekt lineárního zobrazení (a souvislosti mezi nimi) je klíčová tzv. **druhá věta o dimenzi**. Dokážeme si ji pro úplnost textu a její důkaz nebude vyžadován.

Věta 5.18 (2. o dimenzi)**.** *Nechť $A \in \mathcal{L}(P, Q)$. Potom*

$$h(A) + d(A) = \dim P.$$

Důkaz. Nejdříve ukážeme tvrzení pro případ, kdy $h(A) < \infty$ a $d(A) = k < \infty$. Rozlišíme tři možnosti:

1. Pokud $\ker A = P$, potom A zobrazí jakýkoli vektor z P na nulový vektor θ_Q, tedy $h(A) = 0$ a tvrzení triviálně platí.

2. Pokud $\ker A = \{\theta_P\}$ potom A je podle Věty 5.16 prosté zobrazení. Je-li $(x_1, \dots, x_n)$ báze P, potom díky Větě 5.8 soubor $(Ax_1, \dots, Ax_n)$ generuje $A(P)$ a díky Větě 5.16 je tento soubor i lineárně nezávislý. Potom $h(A) = \dim P$ a tvrzení opět platí.

3. Nechť tedy $\ker A \subset\subset P$ je netriviální podprostor. Označme si bázi $\ker A$ jako $(x_1, \dots, x_k)$ a doplňme ji na bázi celého prostoru P přidáním vektorů $(y_1, y_2, \dots, y_n$ Ukážeme, že $(Ay_1, Ay_2, \dots, Ay_{n-k})$ tvoří bázi $A(P)$.

   Nejdříve si dokážeme, že soubor $(Ay_1, Ay_2, \dots, Ay_{n-k})$ generuje $A(P)$:

$$\begin{aligned} A(P) &= A\langle x_1, \dots, x_k, y_1, \dots, y_{n-k}\rangle \\ &= \langle Ax_1, \dots, Ax_k, Ay_1, \dots, Ay_{n-k}\rangle \\ &= \langle Ay_1, \dots, Ay_{n-k}\rangle, \end{aligned}$$

neboť pro každé $i \in \hat{k}$ platí $x_i \in \ker A$, tedy $Ax_i = \theta$.

Zbývá ukázat, že soubor $(Ay_1, Ay_2, \ldots, Ay_{n-k})$ je lineárně nezávislý. Předpokládejme, že

$$\alpha_1 Ay_1 + \cdots + \alpha_{n-k} Ay_{n-k} = \theta.$$

Potom $A(\alpha_1 y_1 + \cdots + \alpha_{n-k} y_{n-k}) = \theta$, neboli $z := \alpha_1 y_1 + \cdots + \alpha_{n-k} y_{n-k} \in \ker A$. Tento vektor lze současně vyjádřit jako kombinaci bázových vektorů $z = \beta_1 x_1 + \cdots + \beta_k x_k$. Vhodným odečtením obdržíme:

$$\theta = z - z = -\beta_1 x_1 - \ldots - \beta_k x_k + \alpha_1 y_1 + \cdots + \alpha_{n-k} y_{n-k}.$$

Z lineární nezávislosti plyne, že všechny koeficienty jsou nulové, neboli $\alpha_i = 0 = \beta_j$ pro $i \in \widehat{n-k}$, $j \in \hat{k}$. Proto je soubor $(Ay_1, \ldots, Ay_{n-k})$ lineárně nezávislý a tvoří bázi $A(P)$.

Konečně dohromady dostáváme

$$h(A) + d(A) = (n-k) + k = \dim P.$$

Zbývá ošetřit případ, kdy se nám na levé straně rovnice objeví ∞ (tzn. $h(A) = \infty$ nebo $d(A) = \infty$). Nejdříve si povšimněme, že jelikož $\ker A$ je podprostorem P, tak jestliže $d(A) = \infty$, pak i $\dim P = \infty$ a dokazovaný vztah platí.

Konečně ukážeme, že je-li $h(A) = \infty$, pak opět $\dim P = \infty$ (a i v tomto případě dokazovaný vztah platí). Pro spor předpokládejme, že $\dim P < \infty$. Potom by existovaly vektory $x_1, \ldots, x_n$ tak, že $P = \langle x_1, \ldots, x_n \rangle$ a díky Větě 5.8 by soubor $(Ax_1, \ldots, Ax_n)$ generoval $A(P)$, což je spor s Důsledkem Steinitzova lemmatu 2.51, ze které plyne $h(A) = \dim A(P) \leq n$. □

Z Vět 5.15 a 5.18 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 5.19. *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 5.20. *Nechť $n \in \mathbb{N}$ a $A \in \mathcal{L}(P_n, Q_n)$. Pak je A injektivní právě tehdy, když je surjektivní.*

[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?

Důkaz. Jelikož $\dim P_n = \dim Q_n = n < \infty$, platí

$$A \text{ je prosté} \Leftrightarrow \ker A = \{\theta_{P_n}\} \Leftrightarrow d(A) = 0 \Leftrightarrow h(A) = n \Leftrightarrow A(P_n) = Q_n \Leftrightarrow A \text{ je na}\,.$$

□

Na závěr této části napravíme hřích z dřívějška. V části 3.4 jsme totiž čtenáře okradli o část důkazu jedné důležité věty, konkrétně šlo o druhou část Frobeniovy věty 3.27. Tuto větu jsme si mohli dokázat již dříve, ale vyžadovalo by to netriviální množství práce. S nově zavedenými pojmy a tvrzeními zvládneme důkaz skoro levou zadní a 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.

Věta 5.21 (Druhá část Frobeniovy věty 3.27)**.** *Buď $\mathbb{A} \in T^{m,n}$, potom pro množinu S_0 všech řešení homogení soustavy $\mathbb{A}\mathbb{x} = \theta$ platí*

$$\dim S_0 = n - h(\mathbb{A})\,.$$

Důkaz. K matici $\mathbb{A} \in T^{m,n}$ definujme zobrazení $A : T^n \to T^m$ 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 $A \in \mathcal{L}(T^n, T^m)$. Zřejmě $\ker A = S_0$, neboť $A\mathbb{x} = \theta \Leftrightarrow \mathbb{A}\mathbb{x} = \theta$.

Lze snadno vypozorovat, že $h(A) = h(\mathbb{A})$, protože

$$A(T^n) = \langle Ae_1, \ldots, Ae_n \rangle^{24} = \langle \mathbb{A}_{:1}, \ldots, \mathbb{A}_{:n} \rangle\,,$$

kde druhá rovnost plyne ze vztahu

$$\begin{aligned} Ae_i &= \mathbb{A} \cdot e_i = \mathbb{A} \cdot (0 \ \cdots \ 0 \ 1 \ 0 \ \cdots \ 0)^T \\ &= 0\mathbb{A}_{:1} + \ldots + 0\mathbb{A}_{:(i-1)} + 1\mathbb{A}_{:i} + 0\mathbb{A}_{:(i+1)} + \ldots + 0\mathbb{A}_{:n} \\ &= \mathbb{A}_{:i} \end{aligned}$$

Přitom platí $\dim\langle \mathbb{A}_{:1}, \ldots, \mathbb{A}_{:n} \rangle = h(\mathbb{A}^T) = h(\mathbb{A})$. Dohromady s druhou větou o dimenzi 5.18 získáváme

$$\dim S_0 = d(A) = n - h(A) = n - h(\mathbb{A}).$$

□

[24] Všichni jistě víme, že $(e_1, \ldots, e_n)$ značí standardní bázi prostoru T^n.

Dodatek k inverzi lineárního operátoru

Ve světě čtvercových matic jsme si již dříve (Věta 3.25) ukázali důležitost vlastnost, a to, že pro existenci inverzní matice (a tedy její regularitu) stačí inverze pouze „z jedné strany“. Posuneme-li se v našich úvahách k lineárním operátorům, obdobné tvrzení platí pouze na prostorech stejné konečné dimenze. Na prostorech nekonečné dimenze lze však alespoň dokázat tvrzení slabší, a to, že z existence „jednostranné inverze“ plyne alespoň jedna z vlastností injektivita, surjektivita. Větu níže zde uvádíme především pro fajnšmekry, nebudeme ji vyžadovat.

Věta 5.22. *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.

*(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 5.20.

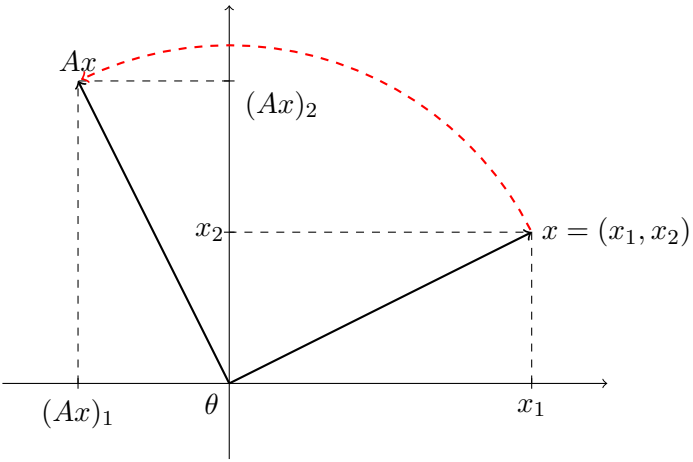
□

5.5 Matice lineárního zobrazení

Jak jsme již naznačili v Poznámce 5.12, 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 $\frac{\pi}{2}$“[25].



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 5.9, 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[26]. Zvolme standardní bázi $\mathbb{R}^2$, $\mathcal{E} = (e_1, e_2) = ((1,0),(0,1))$. Pak platí

$$Ae_1 = A(1,0) = (0,1) = e_2\,, \quad Ae_2 = A(0,1) = (-1,0) = -e_1\,.$$

[25] V kladném smyslu, tedy proti směru hodinových ručiček.

[26] I když u tohoto zobrazení jde o porovnatelně „obtížné“ kroky.

V důkazu druhé části Frobeniovy věty 3.27 , tj. ve Větě 5.21, 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

$$\mathbb{A}\mathbb{e}_j = \mathbb{A}_{:j}\ ^{27}.$$

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 $\mathbb{A} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Nalezenou matici $\mathbb{A}$ budeme posléze sofistikovaněji nazývat *matice zobrazení A ve standardní bázi*[28]. 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

[27] 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 3.10).

[28] Nebo lépe: ze standardní báze do standardní báze.

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[29].

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 5.23. *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 $x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2} \in \mathbb{R}$[30].

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[31] *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*

$$\mathbb{A}\mathbb{X} = A\mathbb{X} \quad \Leftrightarrow \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot \begin{pmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{pmatrix} = \begin{pmatrix} x_{1,1} + x_{1,2} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{pmatrix},$$

[29] Ano, je to děsivě komplikovaná formulace, ale musíme být přesní...

[30] Ověření linearity přenecháváme čtenáři jako minutkové zabavení.

[31] Tedy z definice maticového násobení.

což vede na soustavu lineárních rovnic

$$\begin{aligned}\alpha x_{1,1} + \beta x_{2,1} &= x_{1,1} + x_{1,2}\\ \alpha x_{1,2} + \beta x_{2,2} &= x_{1,2}\\ \gamma x_{1,1} + \delta x_{2,1} &= x_{2,1}\\ \gamma x_{1,2} + \delta x_{2,2} &= x_{2,2}\,.\end{aligned}$$

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*[32]*, 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[33] *jejího obrazu při zobrazení A.*

[32] Pro jednoduchost v té standardní.

[33] Zde opět oboje ve standardní bázi.

Zavedení matice zobrazení

Potřebné značení na téma souřadnice v bázi jsme si zavedli v Definici 2.71, připomeňme si jej. Nechť $\mathcal{X} = (x_1, \ldots, x_n)$ je báze V_n a vektor $z \in V_n$ splňuje vztah $z = \sum_{i=1}^{n} \alpha_i x_i$. **Souřadnicemi vektoru** $z \in V_n$ **v bázi** $\mathcal{X}$ pak rozumíme sloupec

$$(z)_{\mathcal{X}} := \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix},$$

na který lze v případě potřeby pohlížet i jako na obyčejnou $n$tici $(z)_{\mathcal{X}} = (\alpha_1, \ldots, \alpha_n)$. Přiřazení jednotlivé $i$té souřadnice vektoru z v bázi $\mathcal{X}$ pak realizuje tzv. $i$tý souřadnicový funkcionál v bázi $\mathcal{X}$,

$$x_i^{\#}(z) := \alpha_i.$$

Současně z Věty 5.5 víme, že přiřazení souřadnic je samo lineárním zobrazením.

Požadovanou vlastnost hledané matice $\mathbb{A}$ zobrazení $A \in \mathcal{L}(P_m, Q_n)$ v bázích $\mathcal{X}$ a $\mathcal{Y}$ tedy můžeme formulovat stručně jako

$$\forall z \in P : \mathbb{A} \cdot (z)_{\mathcal{X}} = (Az)_{\mathcal{Y}}\,. \tag{5.1}$$

Místo abychom matici zobrazení rovnou definovali[34], zamyslíme se ještě, co pro ni z vlastnosti (5.1) vlastně plyne. Označme vektory standardní báze prostoru T^m zapsané do sloupců jako $\mathbb{e}_1 = (1\ 0\ \cdots\ 0)^T, \ldots, \mathbb{e}_m = (0\ \cdots\ 0\ 1)^T$,[35] 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.[36] Tentýž závěr můžeme učinit i jinak, a to s využitím Věty 2.39. Připomeňme dále, že prvky libovolné báze $\mathcal{X}$ mají vůči této bázi $\mathcal{X}$ speciální tvar! Jelikož zjevně pro každé $j \in \hat{n}$ platí

$$x_j = 0x_1 + \cdots + 0x_{j-1} + 1x_j + 0x_{j+1} + \cdots + 0x_n\,,$$

dostáváme

$$\forall j \in \hat{m} : (x_j)_{\mathcal{X}} = \mathbb{e}_j\,. \tag{5.3}$$

Zkombinujeme-li[37] dohromady rovnosti (5.1), (5.2) a (5.3), dostaneme pro hledanou matici $\mathbb{A}$ rovnost

$$\forall j \in \hat{m} : \mathbb{A}_{:j} = \mathbb{A} \cdot \mathbb{e}_j = \mathbb{A} \cdot (x_j)_{\mathcal{X}} = (Ax_j)_{\mathcal{Y}}\,,$$

[34] Uvádění explicitních definic „natvrdo“, bez předchozích vysvětlení, úvah či příkladů se totiž mezi studenty zdá být velice nepopulární...

[35] Toto značení už jsme dříve několikrát použili.

[36] 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)!

[37] S bonusovou znalostí faktu, že každé lineární zobrazení stačí definovat na vektorech nějaké báze.

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 ${}^{\mathcal{X}}A^{\mathcal{Y}} \in T^{n,m}$ definovanou po sloupcích předpisem*

$$\forall j \in \hat{m} : ({}^{\mathcal{X}}A^{\mathcal{Y}})_{:j} := (Ax_j)_{\mathcal{Y}},$$

*nazveme **maticí zobrazení A v bázích $\mathcal{X}$, $\mathcal{Y}$** (nebo „z báze $\mathcal{X}$ do báze $\mathcal{Y}$").*[38] *Matici lineárního operátoru ${}^{\mathcal{X}}A^{\mathcal{X}}$ zkráceně označíme ${}^{\mathcal{X}}A := {}^{\mathcal{X}}A^{\mathcal{X}}$.*

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 [39]

$$\begin{aligned} A(1,0,0,0) &= (4,1,2)\,,\\ A(0,1,0,0) &= (1,1,3)\,,\\ A(0,0,1,0) &= (0,0,2)\,,\\ A(0,0,0,1) &= (1,2,0)\,, \end{aligned}$$

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 $\mathcal{X} = (x_1, x_2, x_3, x_4)$, $\mathcal{Y} = (y_1, y_2, y_3)$,*

$$x_1 = (2,1,0,0),\ x_2 = (0,2,1,0),\ x_3 = (0,0,2,1),\ x_4 = (1,0,0,2)$$

[38] Pomocí souřadnicového funkcionálu bychom mohli matici zobrazení definovat po jednotlivých prvních takto: $\forall i \in \hat{n}, \forall j \in \hat{m} : {}^{\mathcal{X}}A^{\mathcal{Y}}_{ij} := y_i^{\#}(Ax_j)$.

[39] Jak snadno zjistíme dosazením.

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*[40]

$$\begin{aligned} Ax_1 &= 5y_1 + 3y_2 + y_3, \\ Ax_2 &= -8y_1 + 2y_2 + 8y_3, \\ Ax_3 &= -6y_1 + 2y_2 + 5y_3, \\ Ax_4 &= 5y_2 + y_3. \end{aligned}$$

Odtud dostáváme

$${}^{\mathcal{X}}A^{\mathcal{Y}} = \begin{pmatrix} 5 & -8 & -6 & 0 \\ 3 & 2 & 2 & 5 \\ 1 & 8 & 5 & 1 \end{pmatrix}.$$

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[41] nám pořád zbývá dokázat, že tato podmínka k požadované vlastnosti **postačuje**.

Věta 5.27. *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*

$$(Az)_{\mathcal{Y}} = {}^{\mathcal{X}}A^{\mathcal{Y}} \cdot (z)_{\mathcal{X}}\,,$$

(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*

$(z)_{\mathcal{X}}$ je řešením soustavy lineárních rovnic s rozšířenou maticí $\left({}^{\mathcal{X}}A^{\mathcal{Y}} \,\middle|\, (w)_{\mathcal{Y}}\right)$.

[40] Hledat souřadnice v bázi už samozřejmě dávno umíme.

[41] 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).

Důkaz. (i) Na obou stranách dokazované rovnosti jsou sloupcové vektory z $T^{n,1}$,[42] úpravou součinu napravo dokážeme, že se obě strany rovnají.

Začneme prachobyčejným rozepsáním pravé strany pomocí maticového násobení a následným dosazením, čemu se příslušné prvky v násobených maticích rovnají. Označme $(z)_{\mathcal{X}} = (\alpha_1, \ldots, \alpha_m)$. Využijeme Větu 2.39 (o násobení matice sloupcem zprava) a linearitu obou zobrazení A a $(\cdot)_{\mathcal{Y}}$.

$$\begin{aligned}
{}^{\mathcal{X}}A^{\mathcal{Y}} \cdot (z)_{\mathcal{X}} &= {}^{\mathcal{X}}A^{\mathcal{Y}} \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} \\
&= \sum_{k=1}^{m} \alpha_k \left({}^{\mathcal{X}}A^{\mathcal{Y}}\right)_{:k} \\
&= \sum_{k=1}^{m} \alpha_k \left(Ax_k\right)_{\mathcal{Y}} \\
&= \left(\sum_{k=1}^{m} \alpha_k A x_k\right)_{\mathcal{Y}} \\
&= \left(A\left(\sum_{k=1}^{m} \alpha_k x_k\right)\right)_{\mathcal{Y}} \\
&= (Az)_{\mathcal{Y}} .
\end{aligned}$$

(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 ${}^{\mathcal{X}}A^{\mathcal{Y}} \cdot (z)_{\mathcal{X}} = (w)_{\mathcal{Y}}$.

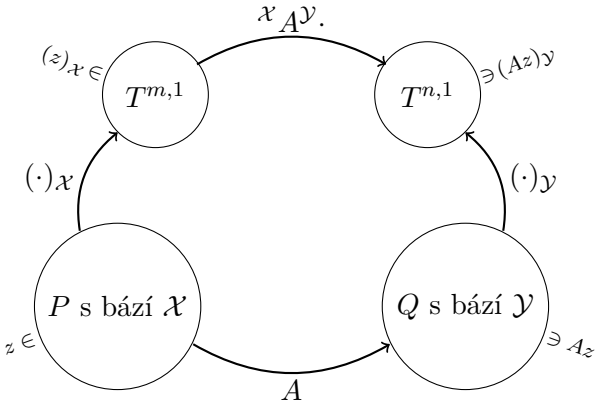
□

Poznámka 5.28. *Věta 5.27 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.*

[42] Upřímně se nad tím zamyslete!



Obrázek 5.2: Schéma, jak „funguje“ matice lineárního zobrazení $A \in \mathcal{L}(P, Q)$.

Jak už víme z dřívějška, přiřazení souřadnic je 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. Navíc pak platí, že množina všech lineárních zobrazení mezi dvěma pevně zvolenými prostory s těmito opracemi tvoří sama vektorový prostor!

Věta 5.29. *Nechť P, Q jsou VP nad T, pro libovolná zobrazení $A, B \in \mathcal{L}(P, Q)$ a $\alpha \in T$ definujeme*

$$\forall x \in P : (A + B)x := Ax + Bx\,, \quad (\alpha A)x := \alpha \cdot Ax\,.$$

Potom platí

$$A + B \in \mathcal{L}(P, Q), \qquad \alpha A \in \mathcal{L}(P, Q)\,.^{43}$$

Důkaz. Ponecháváme čtenáři jako cvičení, uzavřenost množiny $\mathcal{L}(P, Q)$ na sčítání a násobení skalárem lze ověřit přímo z definic. □

Věta 5.30. *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) ${}^{\mathcal{X}}(\alpha A)^{\mathcal{Y}} = \alpha\, {}^{\mathcal{X}}A^{\mathcal{Y}}$.

[43] Dokonce platí, že $(\mathcal{L}(P, Q), T, +, \cdot)$ je vektorovým prostorem! Zkuste si to ověřit.

Důkaz. Obě tvrzení vyplývají z linearity souřadnicových funkcionálů. Porovnáme $j$té sloupce příslušných matic, kde $j \in \hat{m}$ je libovolné:

(i)
$$\begin{aligned}\left({}^{\mathcal{X}}(A+B)^{\mathcal{Y}}\right)_{:j} &= ((A+B)x_j)_{\mathcal{Y}} = (Ax_j + Bx_j)_{\mathcal{Y}} = (Ax_j)_{\mathcal{Y}} + (Bx_j)_{\mathcal{Y}} \\ &= \left({}^{\mathcal{X}}A^{\mathcal{Y}}\right)_{:j} + \left({}^{\mathcal{X}}B^{\mathcal{Y}}\right)_{:j}\end{aligned}$$

(ii)
$$\left({}^{\mathcal{X}}(\alpha A)^{\mathcal{Y}}\right)_{:j} = ((\alpha A)x_j)_{\mathcal{Y}} = (\alpha A x_j)_{\mathcal{Y}} = \alpha\,(Ax_j)_{\mathcal{Y}} = \left(\alpha\ {}^{\mathcal{X}}A^{\mathcal{Y}}\right)_{:j}$$

□

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 5.31. *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 ${}^{\mathcal{X}}(AB)^{\mathcal{W}} \in T^{s,m}$.

Dokážeme, že pro libovolné $j \in \hat{m}$ se $j$té sloupce matic nalevo i napravo rovnají. Kromě hlavní vlastnosti matice zobrazení dále použijeme Definici 3.51, resp. vlastnost (3.7) (která ve zkratce říká, že „$j$tý sloupec součinu $\mathbb{A} \cdot \mathbb{B}$ je roven součinu $\mathbb{A}$ s $j$tým sloupcem $\mathbb{B}$“, to si prosím rozmyslete!).

Nechť $j \in \hat{m}$, pro $j$tý sloupec součinu napravo platí:

$$\begin{aligned}\left({}^{\mathcal{Y}}A^{\mathcal{W}} \cdot {}^{\mathcal{X}}B^{\mathcal{Y}}\right)_{:j} &= {}^{\mathcal{Y}}A^{\mathcal{W}} \cdot \left({}^{\mathcal{X}}B^{\mathcal{Y}}\right)_{:j} \\ &= {}^{\mathcal{Y}}A^{\mathcal{W}} \cdot (Bx_j)_{\mathcal{Y}} \\ &= \left(A(Bx_j)\right)_{\mathcal{W}} \\ &= \left((AB)x_j\right)_{\mathcal{W}} \\ &= {}^{\mathcal{X}}(AB)^{\mathcal{W}}_{:j}.\end{aligned}$$

□

Důsledek 5.32. *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 5.31 pak platí

$${}^{\mathcal{X}}A^{\mathcal{Y}} \,.\, {}^{\mathcal{Y}}(A^{-1})^{\mathcal{X}} = {}^{\mathcal{Y}}(AA^{-1})^{\mathcal{Y}} = {}^{\mathcal{Y}}E^{\mathcal{Y}} = \mathbb{E}\,,$$

kde poslední rovnost plyne z faktu, že vektory libovolné báze $\mathcal{Y} = (y_1, \ldots, y_n)$ splňují[44]

$$\forall j \in \hat{n} : (y_j)_{\mathcal{Y}} = \mathbb{e}_j \quad \Rightarrow \quad {}^{\mathcal{Y}}E^{\mathcal{Y}} = \mathbb{E}\,.$$

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. Před samotným důkazem si ukážeme pomocné tvrzení.

Lemma 5.33. *Nechť $B \in \mathcal{L}(P, Q)$ je izomorfismus a $z_1, \ldots, z_n$ jsou vektory z P, potom platí*

$$\dim\langle z_1, \ldots, z_n\rangle = \dim\langle Bz_1, \ldots, Bz_n\rangle.$$

Důkaz. Je-li $\dim\langle z_1, \ldots, z_n\rangle = k \in \mathbb{N}$[45], potom lze ze souboru $(z_1, \ldots, z_n)$ vybrat kčlenná báze $(z_{i_1}, \ldots, z_{i_k})$ tohoto podprostoru. S pomocí Věty 5.8 získáme

$$\langle Bz_1, \ldots, Bz_n\rangle = B\big(\langle z_1, \ldots, z_n\rangle\big) = B\big(\langle z_{i_1}, \ldots, z_{i_k}\rangle\big) = \langle Bz_{i_1}, \ldots, Bz_{i_k}\rangle.$$

Jelikož soubor $(z_{i_1}, \ldots, z_{i_k})$ je LN a B je injektivní, je díky Větě 5.16 i soubor $(Bz_{i_1}, \ldots, B$ LN. Proto soubor $(Bz_{i_1}, \ldots, Bz_{i_k})$ tvoří bázi $\langle Bz_1, \ldots, Bz_n\rangle$ a konečně získáváme

$$\dim\langle Bz_1, \ldots, Bz_n\rangle = k = \dim\langle z_1, \ldots, z_n\rangle.$$

□

[44] Jak se již stává milou tradicí, čtenář si jistě sám důkladně rozmyslí, proč následující implikace platí, případně si zopakuje významy použitých symbolů...

[45] Rozmyslete si, že je-li $\dim\langle z_1, \ldots, z_n\rangle = 0$, tak tvrzení zřejmě platí.

Věta 5.34. *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

$$h(A) = \dim AP_m = \dim A\langle x_1, \ldots, x_m\rangle = \dim\langle Ax_1, \ldots, Ax_m\rangle.$$

Již víme (Věta 5.5), že přiřazení $z \to (z)_{\mathcal{Y}}$ je lineárním zobrazením (navíc je jak injektivní, tak surjektivní (tedy izomorfismus), jak plyne z našich dosavadních znalostí o souřadnicích v bázi!). Současně z Věty 5.33 víme, že izomorfismus zachovává dimenzi lineárního obalu. Zaměníme-li tedy v lineárním obalu napravo jednotlivé vektory Ax_i jejich souřadnicemi $(Ax_i)_{\mathcal{Y}}$, získáme lineární obal se stejnou dimenzí.

$$\dim\langle Ax_1, \ldots, Ax_m\rangle = \dim\langle (Ax_1)_{\mathcal{Y}}, \ldots, (Ax_m)_{\mathcal{Y}}\rangle.$$

Jenže $n$tice souřadnic $(Ax_1)_{\mathcal{Y}}, \ldots, (Ax_m)_{\mathcal{Y}}$ jsou přímo sloupce matice ${}^{\mathcal{X}}A^{\mathcal{Y}}$, a proto z vlastnosti hodnosti matice platí

$$h(A) = \dim\langle (Ax_1)_{\mathcal{Y}}, \ldots, (Ax_m)_{\mathcal{Y}}\rangle = h({}^{\mathcal{X}}A^{\mathcal{Y}}).$$

□

Důsledek 5.35. *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 5.11 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 5.36. *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 5.37. *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*

$${}^{\mathcal{X}}E^{\mathcal{Y}} \cdot (x)_{\mathcal{X}} = (x)_{\mathcal{Y}}\,,$$

(iii)

$${}^{\mathcal{Y}}E^{\mathcal{Z}} \,.\, {}^{\mathcal{X}}E^{\mathcal{Y}} = {}^{\mathcal{X}}E^{\mathcal{Z}}\,.$$

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 5.32 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 5.27.

(iii) Vyplývá z Věty 5.31.

□

Poznámka 5.38. *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 3.22 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

$$(\mathbb{A} \mid \mathbb{B}) \sim (\mathbb{P}\mathbb{A} \mid \mathbb{P}\mathbb{B}) \overset{\text{pro } \mathbb{A} \text{ reg.}}{\sim} (\mathbb{A}^{-1}\mathbb{A} \mid \mathbb{A}^{-1}\mathbb{B}) = (\mathbb{E} \mid \mathbb{A}^{-1}\mathbb{B})\,. \tag{5.4}$$

Algoritmus 5.39 (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*

$$\begin{aligned} {}^{\mathcal{X}}E^{\mathcal{Y}} &= {}^{\mathcal{E}}E^{\mathcal{Y}} \,.\, {}^{\mathcal{X}}E^{\mathcal{E}} \\ &= ({}^{\mathcal{Y}}E^{\mathcal{E}})^{-1} \,.\, {}^{\mathcal{X}}E^{\mathcal{E}} \,. \end{aligned}$$

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*

$$({}^{\mathcal{Y}}E^{\mathcal{E}} \mid {}^{\mathcal{X}}E^{\mathcal{E}}) \sim (\mathbb{E} \mid ({}^{\mathcal{Y}}E^{\mathcal{E}})^{-1} \,.\, {}^{\mathcal{X}}E^{\mathcal{E}}) = (\mathbb{E} \mid {}^{\mathcal{X}}E^{\mathcal{Y}}) \,.$$

Příklad 5.40. *Uvažujme vektorový prostor $\mathbb{Z}_5^3$ s bázemi*

$$\mathcal{X} = ((1,0,1),(2,0,1),(3,1,0)) \quad a \quad \mathcal{Y} = ((0,1,1),(4,1,0),(2,1,0)) \,,$$

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 5.39 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“[46] a vhodným způsobem použít maticové násobení.

[46] 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.

Hlavní větu této části nepotřebujeme nijak zvlášť dokazovat, je totiž přímým důsledkem Věty 5.31 o matici složeného zobrazení[47].

Věta 5.41. *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*

$$ {}^{\tilde{\mathcal{X}}}A^{\tilde{\mathcal{Y}}} = {}^{\mathcal{Y}}E^{\tilde{\mathcal{Y}}} \,.\, {}^{\mathcal{X}}A^{\mathcal{Y}} \,.\, {}^{\tilde{\mathcal{X}}}E^{\mathcal{X}}. $$

Algoritmus 5.42 (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*

$$ \begin{aligned} {}^{\mathcal{X}}A^{\mathcal{Y}} &= {}^{\mathcal{E}}E^{\mathcal{Y}} \,.\, {}^{\mathcal{X}}A^{\mathcal{E}} \\ &= ({}^{\mathcal{Y}}E^{\mathcal{E}})^{-1} \,.\, {}^{\mathcal{X}}A^{\mathcal{E}} \,. \end{aligned} $$

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*

$$ ({}^{\mathcal{Y}}E^{\mathcal{E}} \mid {}^{\mathcal{X}}A^{\mathcal{E}}) \sim (\mathbb{E} \mid ({}^{\mathcal{Y}}E^{\mathcal{E}})^{-1} \,.\, {}^{\mathcal{X}}A^{\mathcal{E}}) = (\mathbb{E} \mid {}^{\mathcal{X}}A^{\mathcal{Y}}) \,. $$

Příklad 5.43. *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

$$ y_1 = (1,0,1),\ y_2 = (1,1,0),\ y_3 = (1,0,2) \,, $$

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,

$$ {}^{\mathcal{E}_4}A^{\mathcal{E}_3} = \begin{pmatrix} 4 & 1 & 0 & 1 \\ 1 & 1 & 0 & 2 \\ 2 & 3 & 2 & 0 \end{pmatrix} , $$

[47] Což samozřejmě neznamená, že se nad důkazem ani nezamyslíme, ba právě naopak!

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 5.42, 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 [48].

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

$$\mathcal{E} = (e_1, e_2) = ((1,0),(0,1)) ,$$

[48] 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

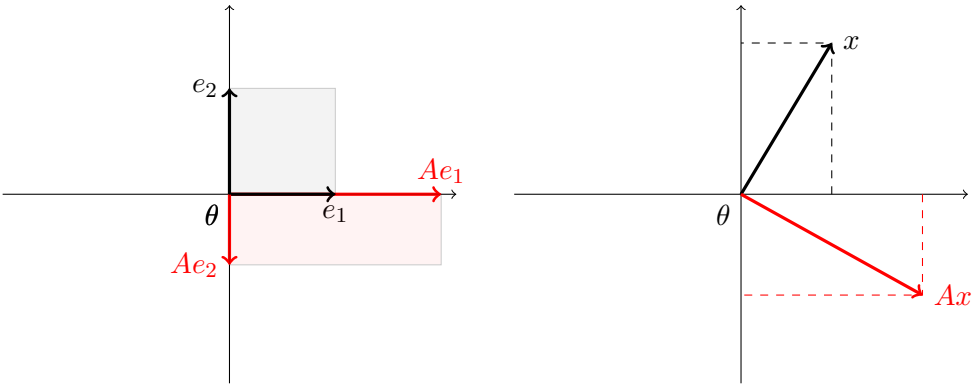
$$ {}^{\mathcal{E}}A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} ,$$

pro kterou z definice platí[49]

$$ {}^{\mathcal{E}}A = \Big((Ae_1)_{\mathcal{E}} \ (Ae_2)_{\mathcal{E}} \Big) .$$

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 5.44 (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 5.3: Operátor škálování podle os s parametry $\alpha = 2, \beta = -\frac{2}{3}$.

Zde snadno odvodíme hledanou matici přímo, každému vektoru v v $\mathbb{R}^2$ zobrazení zřejmě přiřadí

$$(x_1, x_2) \xrightarrow{A} (\alpha x_1, \beta x_2) .$$

Obrazy jednotkových vektorů splňují

$$Ae_1 = \alpha e_1, Ae_2 = \beta e_2 ,$$

[49] Můžeme použít blokový zápis (po sloupcích).

tedy platí

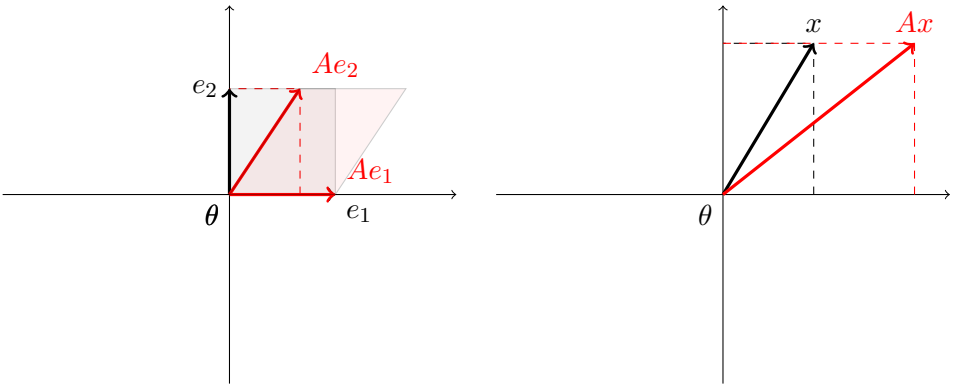
$$\mathcal{E}_A = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}.$$

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

$$\mathcal{E}_{(A^{-1})} = \begin{pmatrix} \frac{1}{\alpha} & 0 \\ 0 & \frac{1}{\beta} \end{pmatrix}^{50}.$$

Příklad 5.45 (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 5.4: 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

$$Ae_1 = e_1, Ae_2 = e_2 + \lambda e_1,$$

[50] 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“).

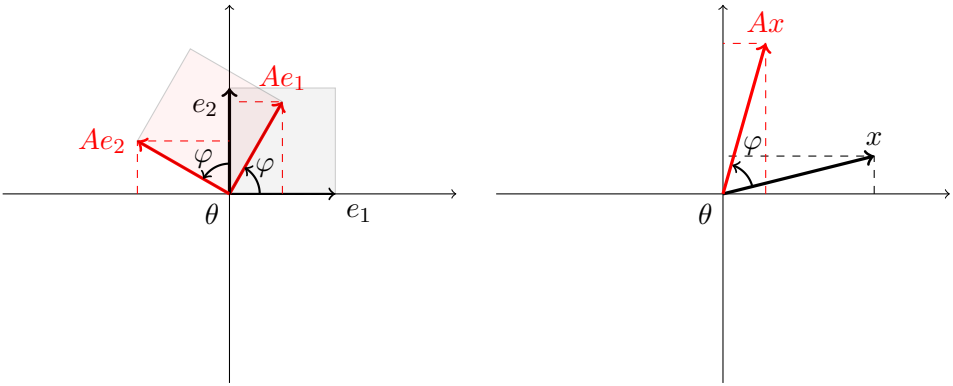
tedy platí

$$ {}^{\mathcal{E}}A = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} . $$

Jak snadno poznáme z tvaru matice ${}^{\mathcal{E}}A$*, zobrazení zkosení je vždy bijekce a příslušné inverzní zobrazení je také zkosením, jeho matice je*

$$ {}^{\mathcal{E}}(A^{-1}) = \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} . $$

Příklad 5.46 (Rotace okolo počátku)**.** *Nechť* $\varphi \in \mathbb{R}$*, uvažujme lineární operátor, který vektory rotuje okolo počátku o úhel* φ *proti směru hodinových ručiček*[51]*.*



Obrázek 5.5: 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[52]*), 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 $(Ax)_{\mathcal{E}} = {}^{\mathcal{E}}A \cdot (x)_{\mathcal{E}}$*, pro obecný vektor platí*

$$ (x_1, x_2) \xrightarrow{A} (x_1\cos\varphi - x_2\sin\varphi, x_1\sin\varphi + x_2\cos\varphi)\,. $$

[51] Jde tedy o přímé zobecnění motivačního příkladu z úvodu části 5.5, kde jsme vektory rotovali o úhel $\varphi = \frac{\pi}{2}$.

[52] Stačí ve znázornění obecného bodu v rovině nalézt vhodný pravoúhlý trojúhelník a zavzpomínat na vlastnosti funkcí sinus a kosinus.

Pro odvození matice inverzního zobrazení můžeme klasicky invertovat matici ${}^{\mathcal{E}}A$*, musíme při tom ale dávat pozor na korektnost prováděných kroků GEM*[53]*! 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*

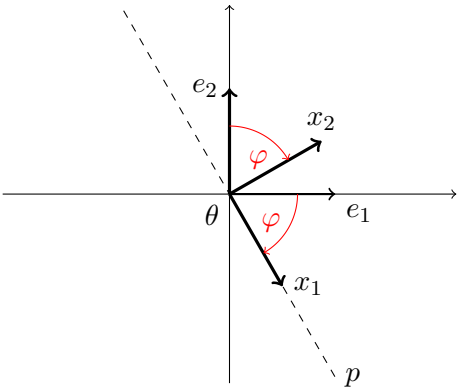
$$ {}^{\mathcal{E}}(A^{-1}) = \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \text{[54]}\,. $$

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[55] 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 5.41.

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 5.46 odvodíme, že vektory této nové báze splňují

$$ \mathcal{X} = (x_1, x_2) = \big((\cos\varphi, \sin\varphi), (-\sin\varphi, \cos\varphi)\big)\,. \tag{5.5} $$

Navíc, jak čtenář jistojistě sám odhalí, není náhodou[56], že matice přechodu ${}^{\mathcal{X}}E^{\mathcal{E}}$ je rovna matici rotace o úhel φ ve standardní bázi.



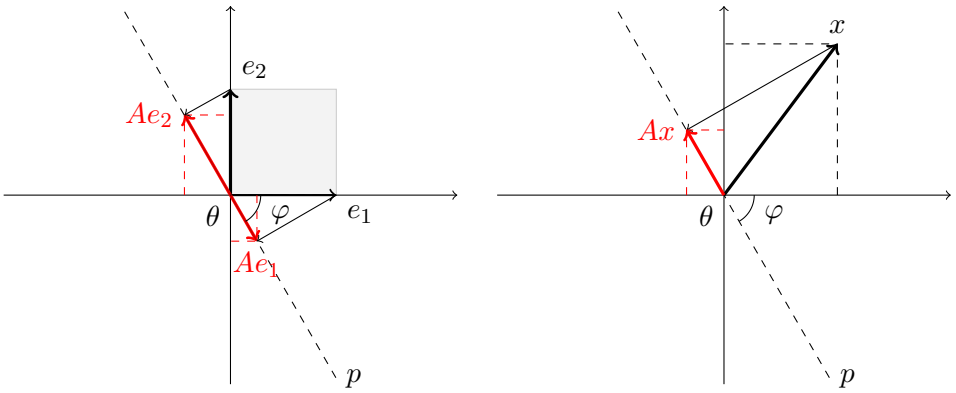
[53] Provádění více kroků najednou v duchu „od $\sin\varphi$násobku jednoho řádku odečtu $\cos\varphi$násobek druhého“ nemusí být korektní a musíme zvažovat různé podmínky pro nenulovost skalárů, jimiž násobíme. Podmínkami vyloučené případy pak musíme ošetřit zvlášť

[54] No a jelikož z žádného našeho kroku nevyplynula žádná podmínka na úhel φ, operátor rotace je vždy bijekcí.

[55] Při dostatku odvahy možná i dvě obecné přímky…

[56] V lineární algebře žádné náhody nemáme.

Příklad 5.47 (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 $v \in \mathbb{R}^2$ přiřadí kolmým promítnutím na přímku p bod na této přímce*[57]*.*



Obrázek 5.6: 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 (5.5) 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 5.41:

$$\begin{aligned} {}^{\mathcal{E}}A &= {}^{\mathcal{X}}E^{\mathcal{E}} \,.\, {}^{\mathcal{X}}A \,.\, {}^{\mathcal{E}}E^{\mathcal{X}} \\ &= {}^{\mathcal{X}}E^{\mathcal{E}} \,.\, {}^{\mathcal{X}}A \cdot ({}^{\mathcal{X}}E^{\mathcal{E}})^{-1} \\ &= \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \\ &= \begin{pmatrix} \cos^2\varphi & \sin\varphi\cos\varphi \\ \sin\varphi\cos\varphi & \sin^2\varphi \end{pmatrix} \end{aligned}$$

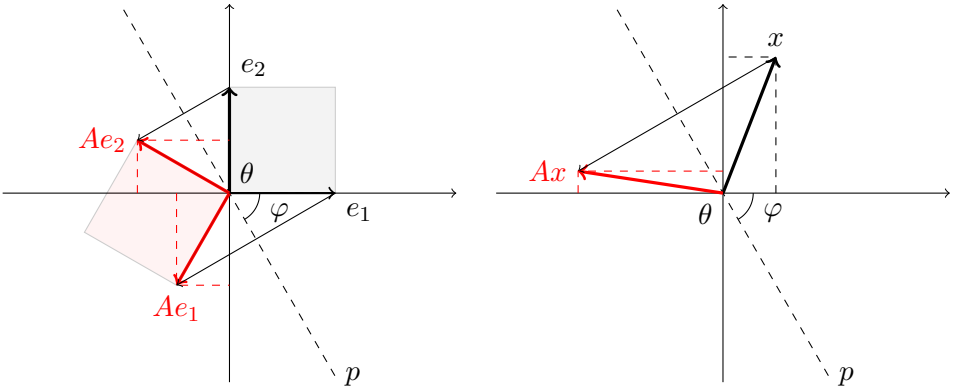
[57] Pojmu „kolmý“ zde rozumíme jaksi naivně, v souladu s tím co známe z hodin klasické rovinné geometrie. Klasikové by snad lépe porozuměli popisu „Z vektoru $x \in \mathbb{R}^2$ spustíme kolmici na přímku p a bod u paty této kolmice pak bude obrazem bodu x.“

a, jelikož se jedná o singulární matici (soubor řádků je vždy LZ), projekce na přímku není nikdy bijekce[58].

Na závěr ještě podotkněme, že získanou matici lze ještě upravit do (pro někoho možná esteticky líbivějšího) tvaru

$$ {}^{\mathcal{E}}A = \begin{pmatrix} \frac{1+\cos(2\varphi)}{2} & \frac{\sin(2\varphi)}{2} \\ \frac{\sin(2\varphi)}{2} & \frac{1-\cos(2\varphi)}{2} \end{pmatrix} $$

Příklad 5.48 (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 5.7: Operátor zrcadlení podle přímky svírající úhel φ s osou x, s parametrem $\varphi = -\frac{\pi}{3}$.

Podobně jako v Příkladu 5.47, namísto geometrického odvozování přejdeme pro jednoduchost k bázi $\mathcal{X}$ zavedené v (5.5) 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 ${}^{\mathcal{E}}A$ od-

[58] Což bychom ostatně mohli odvodit i jednoduchou úvahou o (ne)injektivitě tohoto zobrazení, například odvozením jádra $\ker A$!

vodíme dle Věty 5.41:

$$\begin{aligned}
{}^{\mathcal{E}}A &= {}^{\mathcal{X}}E^{\mathcal{E}} \,.\, {}^{\mathcal{X}}A \,.\, {}^{\mathcal{E}}E^{\mathcal{X}} \\
&= {}^{\mathcal{X}}E^{\mathcal{E}} \,.\, {}^{\mathcal{X}}A \cdot ({}^{\mathcal{X}}E^{\mathcal{E}})^{-1} \\
&= \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \\
&= \begin{pmatrix} \cos^2\varphi - \sin^2\varphi & 2\sin\varphi\cos\varphi \\ 2\sin\varphi\cos\varphi & \sin^2\varphi - \cos^2\varphi \end{pmatrix},
\end{aligned}$$

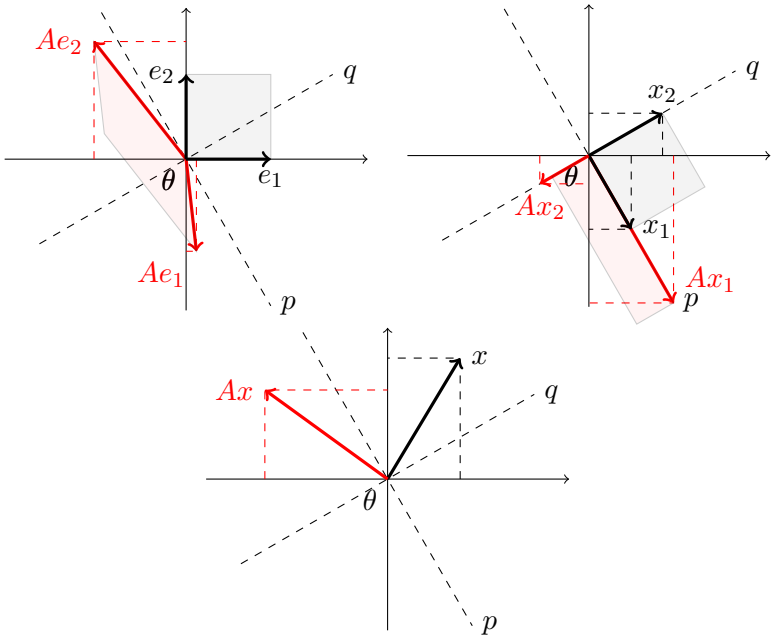
což pomocí známých vzorců rovnou upravíme na

$${}^{\mathcal{E}}A = \begin{pmatrix} \cos(2\varphi) & \sin(2\varphi) \\ \sin(2\varphi) & -\cos(2\varphi) \end{pmatrix}.$$

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[59], můžeme konstatovat, že zrcadlení podle přímky je vždy bijekce a je dokonce samo sobě zobrazením inverzním, tedy $A = A^{-1}$.

Příklad 5.49 (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.*

[59] 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…



Obrázek 5.8: 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 5.41:

$$ \begin{aligned} {}^{\mathcal{E}}A &= {}^{\mathcal{X}}E^{\mathcal{E}} \,.\, {}^{\mathcal{X}}A \,.\, {}^{\mathcal{E}}E^{\mathcal{X}} \\ &= {}^{\mathcal{X}}E^{\mathcal{E}} \,.\, {}^{\mathcal{X}}A \,.\, ({}^{\mathcal{X}}E^{\mathcal{E}})^{-1} \\ &= \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \cdot \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \cdot \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \\ &= \begin{pmatrix} \alpha\cos^2\varphi + \beta\sin^2\varphi & (\alpha-\beta)\sin\varphi\cos\varphi \\ (\alpha-\beta)\sin\varphi\cos\varphi & \alpha\sin^2\varphi + \beta\cos^2\varphi \end{pmatrix} . \end{aligned} $$

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 5.50 (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 5.49 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[60]*, 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

$$ {}^{\mathcal{Y}}E^{\mathcal{E}} = \begin{pmatrix} \cos\varphi & \cos\psi \\ \sin\varphi & \sin\psi \end{pmatrix} $$ [61]

a podobně snadno bychom odvodili i matici zobrazení A v této bázi $\mathcal{Y}$. Matici ve standardní bázi bychom pak získali tradičním postupem,

$$\begin{aligned} {}^{\mathcal{E}}A &= {}^{\mathcal{Y}}E^{\mathcal{E}} \,.\, {}^{\mathcal{Y}}A \,.\, {}^{\mathcal{E}}E^{\mathcal{Y}} \\ &= {}^{\mathcal{Y}}E^{\mathcal{E}} \,.\, {}^{\mathcal{X}}A \cdot ({}^{\mathcal{Y}}E^{\mathcal{E}})^{-1} \\ &= \begin{pmatrix} \cos\varphi & \cos\psi \\ \sin\varphi & \sin\psi \end{pmatrix} \cdot \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \cdot \begin{pmatrix} \cos\varphi & \cos\psi \\ \sin\varphi & \sin\psi \end{pmatrix}^{-1} . \end{aligned}$$

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 5.51. *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*

$$Ax = b\,.$$

[60] V zájmu zachování alespoň malé míry tajemství…

[61] Přičemž o tom, jak obecně vypadá matice k ní inverzní, pomlčíme.

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.

Věta 5.52. *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[62].

Další poznatek, který se týká jádra zobrazení A, už máme také k dispozici, jedná se o *2. větu o dimenzi* (v textu Věta 5.18), kterou zde zopakujeme.

Věta 5.53. *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[63].

Projdeme si několik základních typů rovnic tvaru $Ax = b$.

[62] Žádná velká věda, lineární varietou je libovolná množina ve tvaru „vektor plus podprostor“, ať už v jakémkoli vektorovém prostoru.

[63] V případech, kdy je alespoň jedno z čísel $h(A)$ a $\dim P$ konečné, aby mělo smysl je od sebe odečítat.

Soustavy lineárních rovnic

Předpokládejme, že $P = T^m$ a $Q = T^n$ pro nějaké těleso T a $m, n \geq 1$[64]. 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:

- Množina řešení přidružené homogenní soustavy $A\mathbb{x} = \mathbb{A} \cdot \mathbb{x} = \theta$ je rovna přímo jádru $\ker A$. Pouhým důsledkem Věty 5.52 je pak tvrzení, které říká, že 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 $h(A) = h(\mathbb{A})$, $\dim P = \dim T^m = m$, přímo z 2. věty o dimenzi (jak jsme si již dříve spolu dokázali) plyne druhá část Frobeniovy věty 3.27,

$$h(A) + d(A) = \dim P \quad \Rightarrow \quad h(\mathbb{A}) + \dim S_0 = m \quad \Rightarrow \quad \dim S_0 = m - h(\mathbb{A})\,.$$

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* $S \in \mathcal{L}(T^\infty)$[65] 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[66]

$$\forall k \in \mathbb{N}, \forall n \in \mathbb{N}: (S^k x)_n = x_{n+k}\,.$$

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

$$\forall n \in \mathbb{N}: \;\; A(x_1, x_2, x_3, \dots) := (x_3 - x_2 - x_1, x_4 - x_3 - x_2, x_5 - x_4 - x_3, \dots)$$

[64] Vskutku šokující volba...

[65] S jako posunutí, tedy shift.

[66] Ctihodný čtenář si již jistě stačil zvyknout na to, že výrazy jako *zjevně* nebo *triviálně* jsou diplomatickou zkratkou pro „čtenář si sám dokáže“.

a pro zajímavost uveďme, že například taková Fibonacciho posloupnost[67] 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 $\alpha_0, \ldots, \alpha_k \in T$ a formálně značíme $S^0 = E$.

Rovnici $Ax = b$ pak zapisujeme ve tvaru

$$\forall n \in \mathbb{N} : \ \alpha_k x_{n+k} + \alpha_{k-1} x_{n+k-1} + \cdots + \alpha_1 x_{n+1} + \alpha_0 x_n = b_n \,.$$

Příklad 5.54. *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 $(1-n)_{n\geq 1} = (0, -1, -2, \ldots)$ a poměrně snadno lze uhádnout[68], 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[69] 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, $\forall f \in \mathcal{F} : Df := f'$.

[67] $(1, 1, 2, 3, 5, 8, 13, 21, \ldots)$

[68] Na detaily ohledně tohoto hádání a preciznější postupy zde nemáme prostor. Jsou však stálou náplní kurzu BI-ZDM, Základů diskrétní matematiky.

[69] Hladká funkce je taková která je nejen spojitá, ale navíc k ní existují derivace všech řádů a ty jsou také spojité.

- 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 5.55. *Vyřešíme*[70] *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.

- *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*[71]*, 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*

$$f(x) = 42 + \alpha \cdot e^x \text{ pro nějaké } \alpha \in \mathbb{R}\,.$$

[70] Nicméně velmi ilustračním a neformálním způsobem.
[71] 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 do horního stupňovitého tvaru 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 na „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.

[1] To není žádné velké omezení. Každou konečnou množinu si lze takto očíslovat.

[2] Výslovnost pro našince nepolíbené řečtinou: *pí*, *sigma* a *tau*.

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 $n$tice 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

$$\pi = (3, 1, 5, 2, 4) \quad \text{a} \quad \sigma = (1, 5, 4, 3, 2)$$

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.

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 $\operatorname{sgn} e = (-1)^0 = 1$.*

[3] Skládání zobrazení je asociativní!

Transpozice

Nyní zmíníme speciální jednoduchý druh 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*

$$\begin{vmatrix} 2 & 3 \\ -1 & 1 \end{vmatrix} = 2 \cdot 1 - (-1) \cdot 3 = 2 + 3 = 5.$$

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 $\mathbb{A}$.

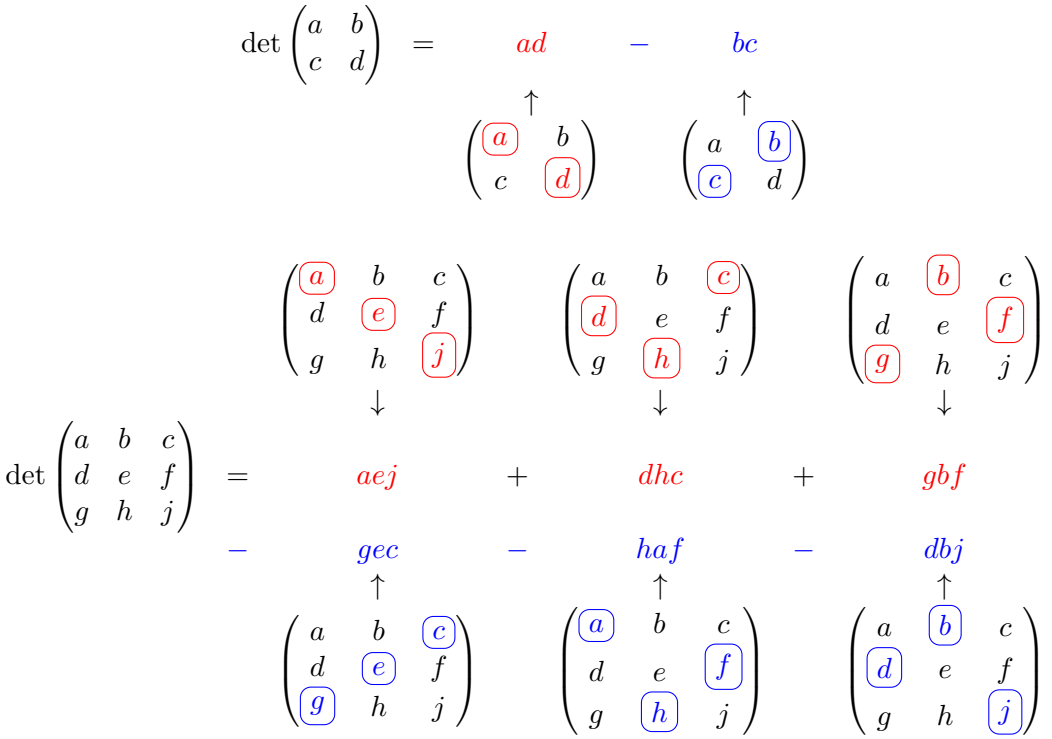
Příklad 6.16. *Platí*

$$\begin{vmatrix} 1 & 2 & 3 \\ 1 & 0 & -1 \\ 3 & 2 & 1 \end{vmatrix} = 0 + 6 - 6 - 0 - (-2) - 2 = 0.$$

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!



Obrázek 6.1: Grafické znázornění křížového a Sarrusova pravidla.

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.

(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. □

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.

[4] Například každá matice $\mathbb{A} \in T^{n,n}$ v horním stupňovitém tvaru je horní trojúhelníková.

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 $i$tého a $j$tého 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 $i$tého 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 $i$tý 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 $i$tého řádku matice, tak toto zobrazení je lineární zobrazení $T^n \to T$. Tj. jsou-li dány $i \in \hat{n}$, řádkové vektory $x_1, \cdots, x_{i-1}, x_{i+1}, x_n$, 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 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. □

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

$$\det \mathbb{B} = \det \mathbb{A} + \det \mathbb{A}' = \det \mathbb{A} + \alpha \det \mathbb{A}'' = \det \mathbb{A} + \alpha \cdot 0 = \det \mathbb{A}.$$

(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.*

[5] Tj. pokud $\alpha = 1$.

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*

$$\det(\mathbb{AB}) = \det \mathbb{A} \cdot \det \mathbb{B}. \tag{6.11}$$

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*

$$\det(\mathbb{PD}) = \det \mathbb{P} \cdot \det \mathbb{D}.$$

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 $\det(\mathbb{PD}) = -\det \mathbb{D}$. 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 $\det(\mathbb{PD}) = \alpha \det \mathbb{D}$. 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.

- $\mathbb{P}$ 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. □

[6] Viz Podkapitola 3.3, část Maticová interpretace GEM.

Důkaz Věty 6.28. Důkaz rozdělíme na dva případy dle regularity matice $\mathbb{A}$.

Nejprve předpokládejme, že matice $\mathbb{A}$ není regulární, tedy $h(\mathbb{A}) < n$. Podle předchozí Věty 6.27 pak platí $\det \mathbb{A} = 0$. Potom z Věty 3.9 plyne, že i

$$h(\mathbb{AB}) \leq h(\mathbb{A}) < n,$$

a tedy součin matic není regulární. Opět dle předchozí Věty 6.27 je $\det(\mathbb{AB}) = 0$. Rovnost (6.11) proto v tomto případě platí ve tvaru $0 = 0$.

Nyní uvažme regulární matici $\mathbb{A}$. Z bodu (iv) Věty 3.20 víme, že $\mathbb{A} \sim \mathbb{E}$. Podle Důsledku 3.18 (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. *Mějme matici $\mathbb{A} \in T^{n,n}$ s prvky a_{ij}[7], kde $n \geq 2$, a $k, \ell \in \hat{n}$. Nechť $\mathbb{A}(k,\ell) \in T^{n-1,n-1}$ je matice, která vznikne z $\mathbb{A}$ vynecháním $k$tého 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)**.** *Mějme matici $\mathbb{A} \in T^{n,n}$ s prvky a_{ij}, kde $n \geq 2$, a $k \in \hat{n}$. 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

$$\mathbb{A}_{:k} = \sum_{i=1}^{n} a_{ik} e_i,$$

kde e_i je $i$tý vektor standardní báze T^n, ekvivalentně podrobněji

$$\begin{pmatrix} a_{1k} \\ a_{2k} \\ \vdots \\ a_{nk} \end{pmatrix} = a_{1k} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \cdots + a_{nk} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Použijeme-li nyní Poznámku 6.22 aplikovanou na $k$tý sloupec matice $\mathbb{A}$, dostaneme

$$\det \mathbb{A} = \sum_{i=1}^{n} a_{ik} \det \mathbb{B}[i,k],$$

[7] V literatuře se toto běžně zapisuje $\mathbb{A} = (a_{ij})$

kde $\mathbb{B}[i,k]$ je matice shodná s maticí $\mathbb{A}$ až na $k$tý sloupec, v němž je vektor e_i, 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[8], celkem se proto determinant při těchto úpravách změní 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. □

Poznámka 6.36. *Jelikož* $\det \mathbb{A} = \det \mathbb{A}^T$*, platí i obdobná věta o rozvoji podle ktého řádku. Výpočet se použitím věty o rozvoji nemusí ve srovnání 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.*

[8] Představte si, že řádek s jedničkou nejprve „probublá“ do prvního řádku a pak sloupec s jedničkou „probublá“ do prvního sloupce.

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)

6.8 Dodatky

Stejně jako dříve přidáváme na závěr pár komentářů a rad navíc, které studentům můžou pomoci rozšířit pochopení látky a lze je občas využít v jiných předmětech.[9] Stejně jako v ostatních kapitolách, látka obsažená v dodatcích nebude vyžádována.

Pro připomenutí: výraz $\mathbb{A}(k, \ell)$ označuje matici, která vznikne z $\mathbb{A}$ vynecháním $k$tého řádku a ℓtého sloupce. Viz Definice 6.34.

Definice 6.39. *Nechť $\mathbb{A} \in T^{n,n}$, $n \geq 2$, matici* $\operatorname{adj} A \in T^{n,n}$ *s prvky*

$$(\operatorname{adj} \mathbb{A})_{ij} = (-1)^{i+j} \det \mathbb{A}(j, i), \;\; i, j \in \hat{n}$$

nazýváme ***adjungovanou maticí*** *k matici $\mathbb{A}$.*

Jinými slovy: adjungovaná matice obsahuje v $i$tém řádku v $j$tém sloupci algebraický doplněk prvku a_{ji}.

Adjungovaná matice je svázaná s původní maticí. Díky ní lze spočítat inverze matic.

Věta 6.40. *Nechť $\mathbb{A} \in T^{n,n}$, kde $n \geq 2$. Potom platí*

$$\mathbb{A} \operatorname{adj} \mathbb{A} = (\det \mathbb{A}) \cdot \mathbb{E}.$$

[9] Například adjungovaná matice se užívá v BI-BEZ.

Důkaz. Chceme ukázat, že $(\mathbb{A}\operatorname{adj}\mathbb{A})_{ij} = ((\det\mathbb{A})\cdot\mathbb{E})_{ij}$ pro všechna $i,j\in\hat{n}$, neboli

$$(\mathbb{A}\operatorname{adj}\mathbb{A})_{ij} = \begin{cases}\det\mathbb{A}, & \text{pokud } i=j,\\ 0, & \text{jinak.}\end{cases}$$

□

Nejdříve si ukážeme první případ:

$$(\mathbb{A}\operatorname{adj}\mathbb{A})_{ii} = \sum_{k=1}^{n}\mathbb{A}_{ik}(\operatorname{adj}\mathbb{A})_{ki} = \sum_{k=1}^{n}\mathbb{A}_{ik}(-1)^{i+j}\mathbb{A}(i,k),$$

což ale dle analogie Věty 6.35 pro řádky přesně odpovídá rozvoji determinantu matice $\mathbb{A}$ podle $i$tého řádku. Proto $(\mathbb{A}\operatorname{adj}\mathbb{A})_{ii} = \det\mathbb{A}$.

Zbývá spočítat $(\mathbb{A}\operatorname{adj}\mathbb{A})_{ij}$, pokud $i\neq j$:

$$(\mathbb{A}\operatorname{adj}\mathbb{A})_{ij} = \sum_{k=1}^{n}\mathbb{A}_{ik}(\operatorname{adj}\mathbb{A})_{kj} = \sum_{k=1}^{n}\mathbb{A}_{ik}(-1)^{i+k}\mathbb{A}(j,k),$$

což ale opět odpovídá rozvoji determinantu matice

$$\mathbb{B} = \begin{pmatrix}\mathbb{A}_{1:}\\ \vdots\\ \mathbb{A}_{j+1:}\\ \mathbb{A}_{i:}\\ \mathbb{A}_{j+1:}\\ \vdots\\ \mathbb{A}_{n:}\end{pmatrix}$$

podle $j$tého řádku. Tato matice $\mathbb{B}$ ale má dva stejné řádky ($i$tý a $j$tý), a proto $(\mathbb{A}\operatorname{adj}\mathbb{A})_{ij} = \det\mathbb{B} = 0$.

Důsledek 6.41. *Nechť $\mathbb{A}\in T^{n,n}$, kde $n\geq 2$, je regulární. Potom inverzní matici lze spočítat předpisem*

$$\mathbb{A}^{-1} = \frac{1}{\det\mathbb{A}}\operatorname{adj}\mathbb{A}.$$

Příklad 6.42. *Máme-li matici regulární matici*

$$\mathbb{A} = \begin{pmatrix}a & b\\ c & d\end{pmatrix},$$

potom pomocí předchozí věty snadno spočítáme inverzní matici

$$\mathbb{A}^{-1} = \frac{1}{ad-bc}\begin{pmatrix}d & -b\\ -c & a\end{pmatrix}.$$

Příklad 6.43. *Aplikujeme-li tuto metodu z Důsledku 6.41 na matici*

$$\mathbb{A} = \begin{pmatrix} 1 & 1 & -2 \\ -1 & -1 & 3 \\ 1 & 2 & -1 \end{pmatrix},$$

obdržíme

$$\mathbb{A}^{-1} = \frac{1}{-1} \begin{pmatrix} (-1)^{1+1}\begin{vmatrix} -1 & 3 \\ 2 & -1 \end{vmatrix} & (-1)^{1+2}\begin{vmatrix} 1 & -2 \\ 2 & -1 \end{vmatrix} & (-1)^{1+3}\begin{vmatrix} 1 & -2 \\ -1 & 3 \end{vmatrix} \\ (-1)^{2+1}\begin{vmatrix} -1 & 3 \\ 1 & -1 \end{vmatrix} & (-1)^{2+2}\begin{vmatrix} 1 & -2 \\ 1 & -1 \end{vmatrix} & (-1)^{2+3}\begin{vmatrix} 1 & -2 \\ -1 & 3 \end{vmatrix} \\ (-1)^{3+1}\begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} & (-1)^{3+2}\begin{vmatrix} -1 & -1 \\ 1 & 2 \end{vmatrix} & (-1)^{3+3}\begin{vmatrix} 1 & 1 \\ -1 & -1 \end{vmatrix} \end{pmatrix}$$

$$= \begin{pmatrix} 5 & 3 & -1 \\ -2 & -1 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Občas nepotřebujeme znát řešení celé, ale stačí nám znát jen některé jeho koeficienty. V tom případě se hodí následující metoda, jak je spočítat.

Věta 6.44 (Cramerovo pravidlo)**.** *Nechť $\mathbb{A} \in \mathbb{R}^n$ je regulární matice a $\mathbb{b} \in T^n$. Potom řešení soustavy $\mathbb{A}\mathbb{x} = \mathbb{b}$, kde $\mathbb{x} = (x_1, \dots, x_n)$, splňuje*

$$x_i = \frac{\det \mathbb{A}_i}{\det \mathbb{A}},$$

kde matice $\mathbb{A}_i$ vznikla z matice $\mathbb{A}$ nahrazením itého sloupce vektorem $\mathbb{b}$, neboli

$$\mathbb{A}_i = \begin{pmatrix} \mathbb{A}_{11} & \mathbb{A}_{12} & \dots & \mathbb{A}_{1\,i-1} & \mathbb{b}_1 & \mathbb{A}_{1\,i+1} & \dots & \mathbb{A}_{1n} \\ \vdots & & & \vdots & \vdots & \vdots & & \vdots \\ \mathbb{A}_{n1} & \mathbb{A}_{n2} & \dots & \mathbb{A}_{n\,i-1} & \mathbb{b}_n & \mathbb{A}_{n\,i+1} & \dots & \mathbb{A}_{nn} \end{pmatrix}.$$

Důkaz. Jelikož $\mathbb{A}$ je regulární z Poznámky 3.28 víme, že existuje právě jedno řešení a to $\mathbb{x} = \mathbb{A}^{-1}\mathbb{b}$. Definujme matici $\mathbb{X} \in T^{n,n}$ předpisem

$$\mathbb{X}_i = (e_1\, e_2 \dots e_{i-1}\, \mathbb{x}\, e_{i+1} \dots e_n),$$

přičemž $e_1, \dots e_n$ jsou prvky standardní báze $\mathcal{E}_n$. Potom s využitím vlastností determinantu obdržíme

$$x_i = \det \mathbb{X}_i = \det(\mathbb{A}^{-1}\mathbb{A}\mathbb{X}_i) = \det(\mathbb{A}^{-1}) \det(\mathbb{A}\mathbb{X}_i)$$

Nyní si zbývá uvědomit, že $\mathbb{A}\mathbb{X}_i = \mathbb{A}_i$:

$$\mathbb{A}\mathbb{X}_i = (\mathbb{A}e_1\, \mathbb{A}e_2 \dots \mathbb{A}e_{i-1}\, \mathbb{A}\mathbb{x}\, \mathbb{A}e_{i+1} \dots \mathbb{A}e_n) = (\mathbb{A}_{:1}\, \mathbb{A}_{:2} \dots \mathbb{A}_{:\,i-1}\, \mathbb{b}\, \mathbb{A}_{:\,i+1} \dots \mathbb{A}_{:,n}) = \mathbb{A}_i.$$

□

V této kapitole jsme pro jednoduchost uvažovali determinant nad $\mathbb{Q}, \mathbb{R}$, či $\mathbb{C}$. Vášnivý čtenář jistě vypozoroval, že jsme pouze v jediném důkazu užili vlastnost těchto čísel a to v případě Důsledku 6.24 (i), který tvrdí „Má-li matice dva stejné řádky, potom je determinant nulový.“. V jeho důkazu kde jsme využili, že z rovnosti $x = -x$ plyne $2x = 0$, a tedy $x = 0$. Tento vztah samozřejmě neplatí v případě $\mathbb{Z}_2$ (a podobných těles). Nicméně Důsledek 6.24 (i) je stále pravdivý, jen v tomto případě je důkaz lehce obtížnější, proto jsme jej v hlavní textu nepoužili.

Důkaz Důsledku 6.24 (i) pro obecné těleso. Mějme matici $\mathbb{A} \in T^{n,n}$, která má stejný $i$tý a $j$tý řádek. Uvažujme permutaci $\pi \in S_n$ k této permutaci existuje právě jedna permutace $\sigma \in S_n$ taková, že $\sigma = \pi \circ \tau_{ij}$. Potom

$$\begin{aligned}
&\operatorname{sgn}(\sigma)\, \mathbb{A}_{1,\sigma(1)}\mathbb{A}_{2,\sigma(2)} \cdots \mathbb{A}_{i,\sigma(i)} \cdots \mathbb{A}_{j,\sigma(j)} \cdots \mathbb{A}_{n,\sigma(n)} \\
&\quad = \operatorname{sgn}(\pi \circ \tau_{ij})\, \mathbb{A}_{1,\pi\circ\tau_{ij}(1)}\mathbb{A}_{2,\pi\circ\tau_{ij}(2)} \cdots \mathbb{A}_{i,\pi\circ\tau_{ij}(i)} \cdots \mathbb{A}_{j,\pi\circ\tau_{ij}(j)} \cdots \mathbb{A}_{n,\pi\circ\tau_{ij}(n)} \\
&\quad = -\operatorname{sgn}(\pi)\, \mathbb{A}_{1,\pi(1)}\mathbb{A}_{2,\pi(2)} \cdots \mathbb{A}_{i,\pi(j)} \cdots \mathbb{A}_{j,\pi(i)} \cdots \mathbb{A}_{n,\pi(n)} \\
&\quad = -\operatorname{sgn}(\pi)\, \mathbb{A}_{1,\pi(1)}\mathbb{A}_{2,\pi(2)} \cdots \mathbb{A}_{i,\pi(i)} \cdots \mathbb{A}_{i,\pi(i)} \cdots \mathbb{A}_{n,\pi(n)}.
\end{aligned}$$

Tedy ke každému sčítanci odpovídajícímu nějaké permutaci existuje právě jedna permutace, jejíž odpovídající sčítanec má opačné znaménko. Tyto sčítance se dohromady sečtou na nulu, a proto je determinant nulový. □

Poznámka 6.45. *Tedy v Definici 6.14 lze uvažovat jakékoliv těleso (klidně i konečné) a tento obecnější determinant bude splňovat všechny vlastnosti uvedené v této kapitole.*[10]

[10] prostě vše včetně vlivu GEMU na determinant, determinant regulární matice, rozvoj determinantu, Cramerova pravidla ....

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 Podkapitola 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

$$ (Ax_1)_{\mathcal{X}} = {}^{\mathcal{X}}A \cdot (x_1)_{\mathcal{X}} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha \\ 0 \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \alpha\,(x_1)_{\mathcal{X}} = (\alpha x_1)_{\mathcal{X}}. $$

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

[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.

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]. 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,

$$({}^{\mathcal{X}}A)^k = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}^k = \begin{pmatrix} \alpha^k & 0 \\ 0 & \beta^k \end{pmatrix}.$$

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***

[5] Vzpomeňte na Příklad č. 5.44

[6] Laskavý čtenář si jistě sám rozmyslí, jak by tato výpočetní porovnání dopadlo v případě $n \times n$ matice.

[7] Řecké písmenko λ, *lambda*.

***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.

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. 5.19; navíc dle Důsledku č. 5.20 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.

[8] Řecké písmenko σ, *sigma*.

[9] Definovaný ovšem na prostoru nekonečné dimenze.

[10] Operátor E označuje identitu na V_n, pro všechna $v \in V_n$ platí $Ev = v$.

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*[11].

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[12]. 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.

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*[13] *ji*[14] *$\nu_g(\lambda)$.*

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[15] 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.

[11] Pozor neplést s vlastním podprostorem z Definice 2.14.

[12] Nezapomínejte, že v této kapitole pracujeme nad tělesem $\mathbb{C}$!

[13] Pozor, v tomto standardním značení je potlačena závislost na A. Při používání tohoto symbolu musí být vždy jasné, o jakém operátoru mluvíme.

[14] Řecké písmenko ν, *ný*.

[15] Vlastní podprostor příslušející vlastnímu číslu λ má dimenzi nejméně 1 a nejvýše n, což je dimenze V_n.

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. 5.30 je ${}^{\mathcal{X}}(A - \lambda E) = {}^{\mathcal{X}}A - \lambda \mathbb{E}$ a proto

$$p_A(\lambda) = \begin{vmatrix} a_{1,1} - \lambda & a_{1,2} & a_{1,3} & \dots & a_{1,n-1} & a_{1,n} \\ a_{2,1} & a_{2,2} - \lambda & a_{2,3} & \dots & a_{2,n-1} & a_{2,n} \\ a_{3,1} & a_{3,2} & a_{3,3} - \lambda & & a_{3,n-1} & a_{3,n} \\ \vdots & \vdots & & \ddots & \vdots & \vdots \\ a_{n-1,1} & a_{n-1,2} & a_{n-1,3} & \dots & a_{n-1,n-1} - \lambda & a_{n-1,n} \\ a_{n,1} & a_{n,2} & a_{n,3} & \dots & a_{n,n-1} & a_{n,n} - \lambda \end{vmatrix}. \tag{7.3}$$

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. 5.41 platí

$${}^{\mathcal{X}}(A - \lambda E) = {}^{\mathcal{Y}}E^{\mathcal{X}} \cdot {}^{\mathcal{Y}}(A - \lambda E) \cdot {}^{\mathcal{X}}E^{\mathcal{Y}}$$

Dále si připomeňme Větu č. 5.37 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[16]

$$p(z) = 2\,(z + 12)(z + 2i)^2(z - 2i)^2(z - 2)^3.$$

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.

Příklad 7.9. *Uvažme operátor A mající v bázi $\mathcal{X}$ prostoru $\mathbb{C}^3$ matici*

$${}^{\mathcal{X}}A = \begin{pmatrix} 1 & -1 & 1 \\ 2 & 0 & -2 \\ 3 & -1 & -1 \end{pmatrix}$$

[16] Snadno ověříte roznásobením.

a nalezněme jeho charakteristický polynom. V závislosti na $\lambda \in \mathbb{C}$ musíme vypočítat následující determinant

$$p_A(\lambda) = \begin{vmatrix} 1-\lambda & -1 & 1 \\ 2 & -\lambda & -2 \\ 3 & -1 & -1-\lambda \end{vmatrix} \overset{1.}{=} \begin{vmatrix} 1-\lambda & -1 & 1 \\ 2-\lambda+\lambda^2 & 0 & -2-\lambda \\ 2+\lambda & 0 & -2-\lambda \end{vmatrix}$$
$$\overset{2.}{=} (-1)^{1+2} \cdot (-1) \cdot \begin{vmatrix} 2-\lambda+\lambda^2 & -2-\lambda \\ 2+\lambda & -2-\lambda \end{vmatrix} \overset{3.}{=} (2+\lambda) \begin{vmatrix} 2-\lambda+\lambda^2 & -2-\lambda \\ 1 & -1 \end{vmatrix}$$
$$\overset{4.}{=} (2+\lambda)(-2+\lambda-\lambda^2+2+\lambda) = \lambda(2+\lambda)(2-\lambda).$$

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. 5.35 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 $\sigma(A)$. □

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[17] η operátoru $A \in \mathcal{L}(V_n)$ je rovna $k \in \hat{n}$. Lze k němu tedy nalézt k lineárně nezávislých vlastních vektorů $v_1, \ldots, v_k$ operátoru A, $Av_j = \eta v_j$ pro každé $j \in \hat{k}$. Doplňme tyto vektory na bázi prostoru V_n,

$$\mathcal{X} = (v_1, \ldots, v_k, v_{k+1}, \ldots v_n).$$

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 $(Av_j)_{\mathcal{X}} = (\eta v_j)_{\mathcal{X}} = (0, \ldots, \eta, \ldots, 0)^T$, kde η je v $j$té složce. Protože podle Lemmatu č. 7.6 charakteristický polynom operátoru A nezávisí na volbě báze, obdržíme rovnost

$$p_A(\lambda) = \det {}^{\mathcal{X}}(A - \lambda E) = \det ({}^{\mathcal{X}}A - \lambda\mathbb{E}).$$

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,

$$p_A(\lambda) = \lambda(2 + \lambda)(2 - \lambda).$$

[17] Řecké písmenko η, *éta*.

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

$$\nu_g(0) = \nu_g(-2) = \nu_g(2) = 1.$$

Příklad 7.14. *Skeptický čtenář by stále mohl mít pochyby o nutnosti pracovat s komplexními čísly. Nejsou příklady operátorů 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[18]*. 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 polynomem 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*[19]

$${}^{\mathcal{X}}A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Jeho charakteristický polynom je roven

$$p_A(\lambda) = \begin{vmatrix} 1-\lambda & 1 \\ 0 & 1-\lambda \end{vmatrix} = (1-\lambda)^2.$$

[18] O tomto operátoru jsme se již zmiňovali v úvodu Podkapitoly 5.5.

[19] Jedná se o operátor zkosení, kterým jsme se zabývali již dříve v Příkladu č. 5.45.

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 ${}^{\mathcal{X}}(A - \lambda_1 E) \cdot (x)_{\mathcal{X}} = \theta$ 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.*

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[20] 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 $\ker(A - \lambda E)$.*

[20] Toto je velmi netriviální krok! Viz Poznámku č. 7.25.

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

$$^{\mathcal{X}}A \cdot (x)_{\mathcal{X}} = \lambda (x)_{\mathcal{X}}.$$

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 $(x)_{\mathcal{X}}$. 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 $(x)_{\mathcal{X}} = \mathbb{x}$.

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 $(\mathbb{A} - \lambda\mathbb{E}) \cdot \mathbb{x} = \theta$.*

Díky tomu, že $\det \mathbb{A} = \det(\mathbb{A} - 0 \cdot \mathbb{E}) = p_{\mathbb{A}}(0)$ dostáme přímo z Věty 6.27 následující pozorování.

Pozorování 7.20. *Matice $\mathbb{A} \in \mathbb{C}^{n,n}$ je regulární, právě když $0 \notin \sigma(\mathbb{A})$.*

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 7.21 (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 matice $\mathbb{A}$.*
3. *Algebraická násobnost vlastního čísla λ, tj. $\nu_a(\lambda)$, je násobnost λ jako kořene charakteristického polynomu $p_{\mathbb{A}}$.*

Algoritmus 7.22 (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 7.23. *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 7.24. *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:

$$\begin{aligned} &\text{pro vlastní číslo } 1: && e_1,\ e_2,\ e_3, \\ &\text{pro vlastní číslo } 2: && e_4,\ e_5, \\ &\text{pro vlastní číslo } 3: && e_6, \end{aligned}$$

kde e_j *označuje* j*tý vektor standardní báze* $\mathbb{C}^6$*. Pro geometrické násobnosti proto platí*

$$\nu_g(1) = 3,\ \nu_g(2) = 2 \text{ a } \nu_g(3) = 1.$$

Poznámka 7.25 (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*[21] *rozměru* $\mathbb{A} \in \mathbb{C}^{100,100}$*. Její charakteristický polynom má stupeň* 100*. Najděte jeho kořeny...*

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[22]*.*

[21] V aplikacích se objevují i matice řádově vyšších rozměrů.

[22] *Plot twist*!

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[23] *předpokládat, že $a_n = 1$. Sestrojme tzv. matici společnici*[24] *$\mathbb{A}_p$ 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.

[23] Dle předpokladu je určitě $a_n \neq 0$ a my řešíme rovnici $p(\lambda) = 0$ což je ekvivalentní $\frac{1}{a_n}p(\lambda) = 0$.

[24] *Companion matrix.*

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 různé matice[25]. 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 7.26. *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 7.27. *Relace podobnosti zavedená v Definici č. 7.26 je relace ekvivalence[26], 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 $\mathbb{D}$.*

Pozorování 7.28. *Jsou-li matice $\mathbb{A}$ a $\mathbb{B}$ podobné, potom mají stejný determinant.*[27]

Důkaz. Mějme regulární matici $\mathbb{P} \in \mathbb{C}^{n,n}$ z definice podobnosti, pak pomocí pravidel pro výpočet determinantu (Věta 6.28 a Důsledek 6.30) získáme

$$\det \mathbb{A} = \det(\mathbb{P}^{-1} \cdot \mathbb{B} \cdot \mathbb{P}) = \det(\mathbb{P}^{-1}) \cdot \det \mathbb{B} \cdot \det \mathbb{P} = (\det \mathbb{P})^{-1} \cdot \det \mathbb{B} \cdot \det \mathbb{P} = \det \mathbb{B}.$$

□

Vztah podobnosti matic přesně vystihuje to, co jsme zmiňovali v úvodním odstavci této podkapitoly. Skutečně, platí totiž následující věta.

[25] Výjimkou je například identický operátor.

[26] S tímto pojmem (relace ekvivalence) se podrobněji setkáte v zimním semestru druhého ročníku v předmětu Základy diskrétní matematiky (BI-ZDM).

[27] Neboli mají-li $\mathbb{A}$ a $\mathbb{B}$ různé determinanty, pak nejsou podobné.

Věta 7.29. *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

$$ {}^{\mathcal{X}}A = \mathbb{A}. $$

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. 5.41 dostáváme

$$ \mathbb{B} = \mathbb{P} \cdot \mathbb{A} \cdot \mathbb{P}^{-1} = {}^{\mathcal{X}}E^{\mathcal{Y}} \,.\, {}^{\mathcal{X}}A \,.\, {}^{\mathcal{Y}}E^{\mathcal{X}} = {}^{\mathcal{Y}}A. $$

$\Leftarrow$: 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. 5.41 platí

$$ \mathbb{A} = {}^{\mathcal{X}}A = {}^{\mathcal{X}}A^{\mathcal{X}} = {}^{\mathcal{Y}}E^{\mathcal{X}} \,.\, {}^{\mathcal{Y}}A^{\mathcal{Y}} \,.\, {}^{\mathcal{X}}E^{\mathcal{Y}} = \mathbb{P}^{-1} \cdot \mathbb{B} \cdot \mathbb{P}, $$

kde jsme označili $\mathbb{P} = {}^{\mathcal{X}}E^{\mathcal{Y}}$. Matice $\mathbb{P}$, jakožto matice přechodu, je regulární. □

Podobné matice mají i „podobné“ vlastnosti. Následující věta nám říká, že mají stejné spektrum a charakteristický polynom. Naopak tedy platí, že pokud matice $\mathbb{A}$ a $\mathbb{B}$ *nemají* stejné spektrum nebo charakteristický polynom, tak *nejsou* podobné.

Věta 7.30. *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. 7.29 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

$$p_{\mathbb{A}}(\lambda) = p_{x_A}(\lambda) = p_{\mathcal{Y}_A}(\lambda) = p_{\mathbb{B}}(\lambda)$$

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 7.31. *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*[28].

Příklad 7.32. *Rozhodněme o podobnosti matic*

$$A = \begin{pmatrix} 87 & 510 \\ -15 & -88 \end{pmatrix} \quad B = \begin{pmatrix} 452 & -1950 \\ 105 & -453 \end{pmatrix}.$$

[28] 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).

Pokusme ověřit přímo podmínku z definice podobnosti (Definice č. 7.26). 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)

$$\begin{pmatrix} 21 & 0 & -108 & 3 \\ 0 & 21 & -102 & -73 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

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. 7.41 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 7.33. *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 7.34. *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 $(x_1, x_2, \ldots$ 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 $(x_1, \ldots, x_j)$. □

Následující věta nejen dává nutnou a postačující podmínku diagonalizovatelnosti operátoru, ale její důkaz[29] i ukazuje jak pak zkonstruovat bázi, vůči níž je daný operátor diagonální.

Věta 7.35 (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 $k \in \hat{n}$, $\lambda_1, \ldots, \lambda_k \in \mathbb{C}$ 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 $\lambda_1, \ldots, \lambda_k$ jsou právě vlastní čísla operátoru A. Jejich algebraické násobnosti jsou popořadě $\ell_1, \ldots, \ell_k$. Konečně i jejich geometrické násobnosti jsou popořadě 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 $\lambda \in \sigma(A)$.

[29] Studujte důkazy!

$\Leftarrow$: 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. 7.34 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[30] $(x_{j,1}, \ldots, x_{j,\ell_j})$ plynou rovnosti

$$\alpha_{j,1} = \alpha_{j,2} = \cdots = \alpha_{j,\ell_j} = 0$$

[30] 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. □

Důsledek 7.36. *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 $\nu_g(\lambda) = \nu_a(\lambda) = 1$. □

Shrňme si v následující poznámce jak diagonalizovat diagonalizovatelný operátor. Stačí jen extrahovat postup z druhé části důkazu Věty č. 7.35.

Poznámka 7.37 (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 7.38 (Diagonalizace matice). *Mějme matici $\mathbb{A} \in \mathbb{C}^{n,n}$ s vlastními čísly $\lambda_1, \dots, \lambda_k$, 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,

$$\mathcal{X} = (\mathbb{x}_{1,1}, \dots, \mathbb{x}_{1,\ell_1}, \mathbb{x}_{2,1}, \dots, \mathbb{x}_{2,\ell_2}, \dots, \mathbb{x}_{k,1}, \dots, \mathbb{x}_{k,\ell_k})$$

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 7.39. *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

$$\begin{aligned} p_{\mathbb{A}}(\lambda) &= \begin{vmatrix} -6-\lambda & -10 & 34 \\ 18 & 22-\lambda & -64 \\ 3 & 5 & -17-\lambda \end{vmatrix} = \begin{vmatrix} -6-\lambda & -10 & 34 \\ 0 & -8-\lambda & 38+6\lambda \\ 3 & 5 & -17-\lambda \end{vmatrix} = \\ &= \frac{1}{3} \begin{vmatrix} 0 & 5\lambda & -\lambda^2-23\lambda \\ 0 & -8-\lambda & 38+6\lambda \\ 3 & 5 & -17-\lambda \end{vmatrix} = \lambda \begin{vmatrix} 5 & -\lambda-23 \\ -8-\lambda & 38+6\lambda \end{vmatrix} = \\ &= \lambda(-\lambda^2-\lambda+6) = -\lambda(\lambda+3)(\lambda-2). \end{aligned}$$

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. 7.36).

Nyní musíme najít příslušné vlastní vektory, tj. nalézt nenulová řešení homogenních soustav $(\mathbb{A} - \lambda_i \mathbb{E}) \cdot \mathbb{x} = \theta$ *pro* $i = 1, 2, 3$. *Uvedeme jen stručně výsledek*[31]

$$\begin{aligned} \text{pro } \lambda_1 = 0: &\quad (9, -19, -4), \\ \text{pro } \lambda_2 = 2: &\quad (2, -5, -1), \\ \text{pro } \lambda_3 = -3: &\quad (2, -4, -1). \end{aligned}$$

Matice $\mathbb{P}$, *pro kterou platí*

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -3 \end{pmatrix} = \mathbb{P}^{-1} \cdot \mathbb{A} \cdot \mathbb{P}$$

proto je

$$\mathbb{P} = \begin{pmatrix} 9 & 2 & 2 \\ -19 & -5 & -4 \\ -4 & -1 & -1 \end{pmatrix}.$$

Příklad 7.40. *Rozhodněte o diagonalizovatelnosti matice*

$$\mathbb{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix}.$$

Abychom mohli využít Větu č. 7.35 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*

$$\mathbb{A} - \lambda_1 \mathbb{E} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix},$$

[31] Řešení soustav lineárních rovnic už máme touto dobou v malíčku.

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. 7.35 není diagonalizovatelná.*

Příklad 7.41. *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. 7.32 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*[32]. *Spočtěme vlastní vektory, uvedeme jen stručně výsledky. Pro matici* $\mathbb{A}$ *jsou vlastními vektory*

$$\begin{aligned} \lambda_1 = -3: &\qquad v_1 = (17,-3), \\ \lambda_2 = 2: &\qquad v_2 = (6,-1), \end{aligned}$$

a pro matici $\mathbb{B}$ *máme*

$$\begin{aligned} \lambda_1 = -3: &\qquad u_1 = (30,7), \\ \lambda_2 = 2: &\qquad u_2 = (13,3). \end{aligned}$$

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):

$$\begin{pmatrix} -3 & 0 \\ 0 & 2 \end{pmatrix} = \mathbb{P}_{\mathbb{A}}^{-1} \cdot \mathbb{A} \cdot \mathbb{P}_{\mathbb{A}} = \mathbb{P}_{\mathbb{B}}^{-1} \cdot \mathbb{B} \cdot \mathbb{P}_{\mathbb{B}}, \tag{7.9}$$

[32] Pokud matice nejsou podobné, pak tento postup bude pravděpodobně výrazně jednodušší než ověřování pomocí definice.

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)

$$\mathbb{A} = (\mathbb{P}_{\mathbb{B}} \cdot \mathbb{P}_{\mathbb{A}}^{-1})^{-1} \cdot \mathbb{B} \cdot (\mathbb{P}_{\mathbb{B}} \cdot \mathbb{P}_{\mathbb{A}}^{-1}).$$

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 7.42. *Pokud jsou dvě matice podobné stejné diagonální matici potom díky Větě č. 7.27 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.*

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

$$F_n = F_{n-1} + F_{n-2}, \quad n = 3, 4, 5, \ldots \tag{7.10}$$

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[33]?

[33] Vyzýváme čtenáře, aby na tomto místě zkusil zformulovat hypotézu o rychlosti růstu $(F_n)_{n=1}^{\infty}$. Roste polynomiálně, exponenciálně, jako faktoriál, nebo jinak?

Klíčovým východiskem k zodpovězení těchto otázek je přeformulování rekurentního vztahu (7.10) do maticového tvaru. Utvořme sloupcový vektor $\mathbb{f}_n = \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix}$, $n = 2, 3, \ldots$, 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 $n = 2, 3, 4, \ldots$ 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

$$\mathbb{f}_n = \mathbb{A}^{n-2} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad n = 2, 3, 4, \ldots \tag{7.11}$$

Spočtěme **vlastní čísla** a vektory matice $\mathbb{A}$. Pro charakteristický polynom matice $\mathbb{A}$ platí

$$p_{\mathbb{A}}(\lambda) = \begin{vmatrix} 1-\lambda & 1 \\ 1 & -\lambda \end{vmatrix} = \lambda^2 - \lambda - 1.$$

Jeho kořeny jsou reálná čísla[34]

$$\lambda_{\pm} = \frac{1}{2}\left(1 \pm \sqrt{5}\right).$$

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

$$\mathbb{P} = (v_+^T\, v_-^T) = \begin{pmatrix} \lambda_+ & \lambda_- \\ 1 & 1 \end{pmatrix} \quad \text{a} \quad \mathbb{P}^{-1} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & -\lambda_- \\ -1 & \lambda_+ \end{pmatrix}.$$

[34] Číslo $\varphi = \frac{1+\sqrt{5}}{2}$ je známé pod názvem „zlatý řez“.

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

$$F_n = \frac{1}{\sqrt{5}}(\lambda_+^n - \lambda_-^n). \tag{7.12}$$

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.

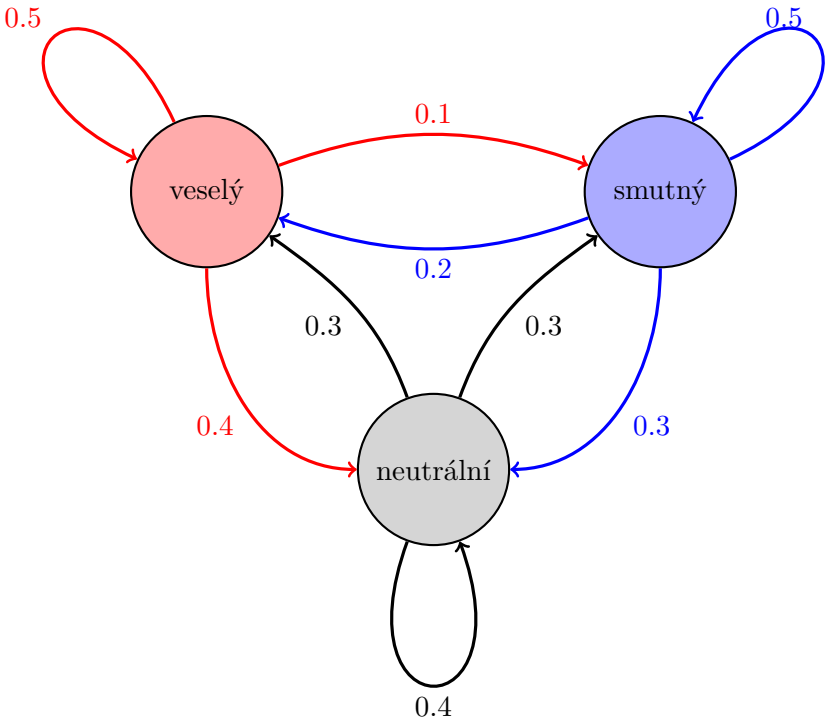
$$\lim_{n\to\infty} \frac{\frac{1}{\sqrt{5}}\lambda_+^n}{F_n} = 1.$$

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.

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[35]. 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.

[35] Andrey Andreyevich Markov, ruský matematik, 1856–1922.



Obrázek 7.1: Denní mentální stavy Pepy Vomáčky a pravděpodobnosti přechodu mezi nimi.

V této podkapitole nebudeme zacházet příliš do detailů a k demonstraci takovéhoto systému použijeme jednoduše uchopitelný a představitelný příklad[36]. 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[37] $\mathbb{P} \in \mathbb{R}^{3,3}$ jejíž prvek $\mathbb{P}_{ij}$ udává pravděpodobnost

[36] Příklad je převzat z monografie *Introduction to Probability Models* od S.M. Rosse. Na markovské řetězce lze narazit i v řadě skutečně praktických úloh.

[37] 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[38]

$$\mathbb{P} = \begin{pmatrix} 0.5 & 0.3 & 0.2 \\ 0.4 & 0.4 & 0.3 \\ 0.1 & 0.3 & 0.5 \end{pmatrix}.$$

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[39] 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 $\{X_j\}_{j=1}^n$)

$$\bar{X} := \frac{1}{n} \sum_{j=1}^{n} X_j \in \mathbb{R}^k.$$

[38] Matice $\mathbb{P}$ je tzv. stochastická: její prvky jsou nezáporná čísla a součet v každém sloupečku je roven 1.

[39] 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.

Dále sestavíme **kovarianční matici** $\mathbb{A} \in \mathbb{R}^{k,k}$ jejíž prvky splňují

$$\mathbb{A}_{i\ell} = \frac{1}{n} \sum_{j=1}^{n} (X_{j,i} - \bar{X}_i)(X_{j,\ell} - \bar{X}_\ell).$$

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[40], 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

$$u_1 = (5.45123, 5.33731)^T \quad \text{a} \quad u_2 = (1.58255, -1.61633)^T.$$

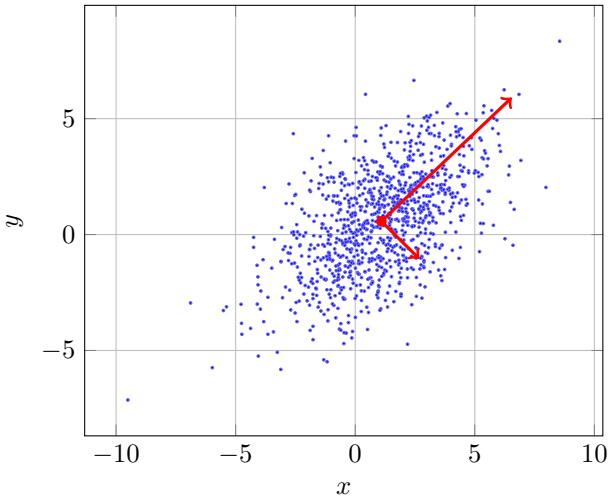
Vlastní vektory jsme naškálovali tak, aby měly délku rovnu právě příslušnému vlastnímu číslu.

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.

7.6 Dodatek: kam dál?

Na závěr uvedeme pouze několik poznámek doplňující výklad v této kapitole.

[40] Nenulový násobek vlastního vektoru je stále vlastní vektor příslušející stejnému vlastnímu číslu.



Obrázek 7.2: Sada dat (modré body) a „hlavní komponenty“ (červené šipky).

Poznámka 7.43 (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 7.44 (*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[41] *matice* $\mathbb{U} \in \mathbb{C}^{m,m}$, $\mathbb{V} \in \mathbb{C}^{n,n}$ *a diagonální*[42] *matice* $\mathbb{S} \in \mathbb{C}^{m,n}$ *splňující*[43]

$$\mathbb{A} = \mathbb{U} \cdot \mathbb{S} \cdot \overline{\mathbb{V}^T}.$$

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).

[41] Unitární matice je regulární matice jejíž sloupce jsou na sebe vzájemně kolmé a jsou normalizované na jedničku (vzhledem ke standardnímu skalárnímu součinu na $\mathbb{C}^n$).

[42] Pouze prvky $\mathbb{S}_{jj}$ mohou být nenulové.

[43] Pruh nad maticí označuje komplexní sdružení všech prvků příslušné matice.

Kapitola 8

Skalární součin a ortogonalita

V této závěrečné kapitole studijního textu BI-LIN se budeme věnovat pojmům skalární součin a ortogonalita a několika zajímavým navazujícím tvrzením. V letním semestru 2018/19 je u zkoušek vyžadovaná pouze jeho část, a to celá podkapitola Skalární součin a částečně Ortogonalita, konkrétně po Větu 8.15 s důkazem včetně. [1]

Co do množství textu je tato kapitola spíše „hubenější“, štědřejší rozepisování je v plánu v příštích letech![2]

S pojmy skalární součin či kolmost se ctihodný čtenář jistě setkal již na střední škole, a to při řešení standardních geometrických úloh v rovině či prostoru. Aniž by věděl, naučil se tak pracovat s tzv. *standardním skalárním součinem ve vektorových (prehilbertových) prostorech* $\mathbb{R}^2$ *a* $\mathbb{R}^3$. Slovo *vektor* přitom chápal jako bod nebo šipku a dále pracoval s pojmy *úhel* svíraný vektory či přímkami a *velikost* vektoru[3]. My si všechny tyto pojmy zavedeme pěkně obecně a namísto řešení geometrických úloh se vydáme spíše teoretickým směrem.

8.1 Co si z této kapitoly odneseme

1. Zavedení pojmu skalární součin a norma ve vektorovém prostoru.
2. Odvození několika jejich užitečných vlastností, definici úhlu.
3. Definici ortogonálního (OG) a ortonormálního (ON) souboru vektorů a pochopení, proč je výhodné pracovat s OG/ON soubory a bázemi.
4. Symetrické matice mají ON bázi tvořenou vlastními vektory.

[1] Platí i pro studenty v LS 2020/21.
[2] Vzhledem k nové akreditaci asi nic takového nenastane.
[3] Které my budeme, obecněji, říkat *norma*!

8.2 Skalární součin

Jak již bylo naznačeno v úvodu, skalární součin není jen ta jedna „středoškolská formulka“, jedná se o mnohem obecnější pojem.

Definice 8.1. *Buď V VP nad $T \subseteq \mathbb{C}$. Zobrazení $(\cdot,\cdot) : V \times V \to T$ nazýváme **skalární součin**, platí-li pro každé vektory $x, y, z \in V$ a každý skalár $\alpha \in T$ následující axiomy:*

1. $(x, \alpha y + z) = \alpha(x, y) + (x, z)$, *(linearita v druhém argumentu[4])*
2. $(x, y) = \overline{(y, x)}$,[5] *(hermitovská symetrie)*
3. $(x, x) \geq 0$ *a zároveň* $\big((x, x) = 0 \Leftrightarrow x = \theta\big)$. *(pozitivní definitnost)*

*Dvojici $(V, (.,.))$ nazýváme **prostorem se skalárním součinem (prehilbertův prostor)** a značíme $\mathcal{H}$.*

Poznámka 8.2. *Upozorňujeme čtenáře na další[6] zákeřnost ve značení, které se ovšem dá jen těžko vyhnout. Spatříte-li tedy výraz typu (x, y) pro $x, y \in V$, mějte se na pozoru, abyste z kontextu poznali, jedná-li se o soubor dvou vektorů nebo o jejich skalární součin.*

Poznámka 8.3. *Je-li $T = \mathbb{R}$, potom $\overline{(y, x)} = (y, x)$,[7] a tedy 2. axiom lze přepsat do tvaru $(x, y) = (y, x)$ (symetrie), neboli opruhování je v $\mathbb{R}$ nadbytečné.*

V libovolném vektorovém prostoru se skalárním součinem platí následující jednoduché vlastnosti, které lze dokázat přímo z definice skalárního součinu.

Pozorování 8.4. *Pro libovolné $x, y, z \in \mathcal{H}$ a $\alpha \in T$ platí*

1. $(\alpha x + y, z) = \overline{\alpha}(x, z) + (y, z)$,
2. $(x, \theta) = (\theta, x) = 0$.

Důkaz.

1. $(\alpha x + y, z) \overset{\text{ax. 2.}}{=} \overline{(z, \alpha x + y)} \overset{\text{ax.1.}}{=} \overline{\alpha(z, x) + (z, y)} \overset{\text{vlastnost } \overline{z}}{=} \overline{\alpha}\overline{(z, x)} + \overline{(z, y)} \overset{\text{ax. 2.}}{=} \overline{\alpha}(x, z) + (y, z)$.
2. $\overline{(\theta, x)} \overset{\text{ax. 2.}}{=} (x, \theta) = (x, (-1)x + x) \overset{\text{ax. 1.}}{=} (-1)(x, x) + (x, x) = 0$.

□

[4] Pozorování 5.6 nám dává, že pro libovolný vektor x je zobrazení $A(\cdot) = (x, \cdot)$ lineární.

[5] Je-li $z = a + bi$ komplexní číslo, potom komplexně sdružené číslo $\overline{z}$ je definováno předpisem $\overline{z} = a - bi$.

[6] Ano, již nekolikátou.

[7] Pro každé reálné číslo a je $\overline{a} = a$.

Konečně si můžeme uvést několik příkladů skalárních součinů.

Příklad 8.5.

- *Na T^n definujeme*
$$(x, y) := \sum_{j=1}^{n} \overline{\xi}_j \eta_j,$$
*kde $x = (\xi_1, \ldots, \xi_n)$, $y = (\eta_1, \ldots, \eta_n)$. Tento skalární součin nazýváme **standardním skalárním součinem**.*

- *Pro $f, g \in C(\langle 0, 1\rangle)$ (spojité funkce) je zobrazení definované vztahem*
$$(f, g) := \int_0^1 \overline{f(x)} g(x) dx$$
skalárním součinem na VP $C(\langle 0, 1\rangle)$.

- *Další příklad skalárního součinu je např. zobrazení definované na prostoru matic $\mathbb{C}^{n,n}$,*
$$(\mathbb{A}, \mathbb{B}) := \sum_{i=1}^{n} \sum_{j=1}^{n} \overline{a}_{i,j} b_{i,j}.$$

- *Na $\mathbb{R}^2$ můžeme definovat i jiný než standardní skalární součin, např.*
$$(x, y) := \begin{pmatrix} \xi_1 & \xi_2 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} \eta_1 \\ \eta_2 \end{pmatrix} = 2\xi_1\eta_1 + \xi_1\eta_2 + \xi_2\eta_1 + \xi_2\eta_2,$$
kde $x = (\xi_1, \xi_2)$, $y = (\eta_1, \eta_2)$.

Pomocí skalárního součinu definujeme pojem norma.

Definice 8.6. *Buď $\mathcal{H}$ prostor se skalárním součinem. Zobrazení $\|.\| : \mathcal{H} \to T$ definované vztahem*
$$\forall x \in \mathcal{H} : \|x\| := \sqrt{(x, x)}$$
*nazýváme **normou** na $\mathcal{H}$.*

Poznámka 8.7. *Máme-li $\mathbb{R}^3$ se standardním skalárním součinem, $\|x\|$ je velikost vektoru x, tj. (eukleidovská) vzdálenost bodu $x = (x_1, x_2, x_3)$ od počátku θ. Z tohoto pohledu lze normu vektoru chápat jako zobecněnou velikost vektoru.*
Podobně je číslo $\|x - y\|$ zobecněnou vzdáleností vektorů x a y.

Následující pozorování si pečlivý čtenář jistě snadno dokáže sám, vystačí si s axiomy skalárního součinu a definicí normy.

Pozorování 8.8. *Pro libovolné $x \in \mathcal{H}$ a $\alpha \in T$ platí:*

1. $\|x\| \geq 0$,
2. $\|x\| = 0 \Leftrightarrow x = \theta$,
3. $\|\alpha x\| = |\alpha| \cdot \|x\|$.

S trojúhelníkovou nerovností se student již pravděpodobně dříve setkal v geometrii, u trojúhelníků v $\mathbb{R}^2$. My si dokážeme její přirozené zobecnění pro libovolný prehilbertův prostor, spolu s dalším důležitým vztahem, Schwarzovou nerovností.

Věta 8.9. *Buď $\mathcal{H}$ prehilbertův prostor. Potom pro $x, y \in \mathcal{H}$ platí:*

1.
$$|(x,y)| \leq \|x\| \cdot \|y\|, \qquad \textit{(Schwarzova nerovnost)}$$
2.
$$\|x+y\| \leq \|x\| + \|y\|, \qquad \textit{(trojúhelníková nerovnost)}$$

Důkaz.

1. Pro $x = \theta$ platí ve Schwarzově nerovnosti rovnost. Uvažujme $x \neq \theta$. Nechť $\lambda \in T$. Potom platí
$$\begin{aligned} 0 \leq (\lambda x - y, \lambda x - y) &= \|\lambda x\|^2 - (\lambda x, y) - (y, \lambda x) + \|y\|^2 \\ &= |\lambda|^2 \|x\|^2 + \|y\|^2 - 2\mathrm{Re}\,\overline{\lambda}(x,y) \end{aligned}$$
pro všechna $\lambda \in T$. Nyní volme speciálně
$$\lambda := \frac{(x,y)}{\|x\|^2},$$
Pro takto zvolené λ máme
$$\frac{|(x,y)|^2}{\|x\|^4}\|x\|^2 + \|y\|^2 - 2\mathrm{Re}\,\frac{|(x,y)|^2}{\|x\|^2} \geq 0,$$
a tedy[8]
$$\|y\|^2 - \frac{|(x,y)|^2}{\|x\|^2} \geq 0,$$
z čehož vyplývá Schwarzova nerovnost.

[8] Jelikož podíl $\frac{|(x,y)|^2}{\|x\|^2}$ je reálné číslo, je rovno své reálné části.

2. Máme

$$\begin{aligned}\|x+y\|^2 &= (x+y, x+y) = (x,x) + (x,y) + (y,x) + (y,y)\\ &= \|x\|^2 + (x,y) + \overline{(x,y)} + \|y\|^2 = \|x\|^2 + 2\mathrm{Re}\,(x,y) + \|y\|^2\end{aligned}$$

Nyní stačí na člen $\mathrm{Re}\,(x,y)$ použít odhad $\mathrm{Re}\,z \le |z|$, který platí pro $\forall z \in \mathbb{C}$, a poté Schwarzovu nerovnost, tj.

$$\mathrm{Re}\,(x,y) \le |(x,y)| \le \|x\|\|y\|.$$

Celkem dostáváme

$$\|x+y\|^2 \le \|x\|^2 + 2\|x\|\|y\| + \|y\|^2 = (\|x\| + \|y\|)^2,$$

což po odmocnění levé a pravé strany dává trojúhelníkovou nerovnost.

□

Pomocí skalárního součinu můžeme zobecnit pojmy úhel přímek a vektorů, které doposud známe z prostorů $\mathbb{R}^2$ nebo $\mathbb{R}^3$ (se standardním skalárním součinem).

Definice 8.10. *Buď $\mathcal{H}$ prehilbertův prostor*[9].

*a) Buďte $\theta \neq x, y \in \mathcal{H}$. **Úhlem vektorů** x, y nazýváme číslo*

$$\arccos \frac{Re\,(x,y)}{\|x\|\|y\|}.$$

Tedy úhel dvou vektorů je z intervalu $\langle 0, \pi\rangle$.

*b) Buďte p, q přímky v $\mathcal{H}$. **Úhlem přímek** p, q nazýváme číslo*

$$\arccos \frac{|Re\,(s_p, s_q)|}{\|s_p\|\|s_q\|},$$

kde s_p (resp. s_q) je směrový vektor přímky p (resp. q). Tedy úhel dvou přímek je z intervalu $\langle 0, \pi/2\rangle$.

Poznámka 8.11.

1. *Podle Schwarzovy nerovnosti platí*

$$-1 \le \frac{Re\,(x,y)}{\|x\|\|y\|} \le 1,$$

tedy výrazy v definici mají smysl.

2. *Úhel přímek nezávisí na volbě směrových vektorů.*

[9] Pokud má čtenář fobii z komplexních čísel a bude pracovat pouze nad tělesem $\mathbb{R}$, může si v této definici odmyslet reálnou část Re.

8.3 Ortogonalita

Nyní si zavedeme pojem ortogonalita (kolmost) souboru vektorů. Máme-li $\mathbb{R}^2$ se standardním skalárním součinem, je „klasická geometrická kolmost“ vektorů x a y ekvivalentní rovnosti $(x, y) = 0$. Tuto vlastnost zobecníme na soubory vektorů libovolné délky v libovolném prehilbertově prostoru.

Definice 8.12. *Nechť $\mathcal{H}$ je prostor se skalárním součinem. Vektory $x, y \in \mathcal{H}$ nazýváme **ortogonální (kolmé)**, právě když $(x, y) = 0$.*[10]

*Soubor vektorů $(x_1, \ldots, x_n)$ z $\mathcal{H}$ nazveme **ortogonální** (OG), právě když*

$$\forall i, j \in \hat{n}, i \neq j : (x_i, x_j) = 0.$$

*Soubor vektorů $(x_1, \ldots, x_n)$ z $\mathcal{H}$ nazveme **ortonormální** (ON), právě když*

$$\forall i, j \in \hat{n} : (x_i, x_j) = \delta_{ij}.$$[11]

Poznámka 8.13. *Z definice plyne, že ortonormální soubor je právě takový soubor vektorů, který je ortogonální a zároveň všechny jeho vektory mají velikost 1.*

I v obecném prehilbertově prostoru $\mathcal{H}$ platí známá Pythagorova věta.

Věta 8.14 (Pythagorova věta)**.** *Nechť (x, y) je OG soubor vektorů z $\mathcal{H}$. Potom*

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2.$$

Důkaz. Platí

$$\|x + y\|^2 = (x + y, x + y) = \|x\|^2 + (x, y) + (y, x) + \|y\|^2.$$

Nyní stačí využít, že dle předpokladu je $0 = (x, y) = (y, x)$. □

Věta 8.15. *OG soubor **nenulových** vektorů je LN. Speciálně, každý ON soubor vektorů je LN.*

Důkaz. Buď $(x_1, \ldots, x_n)$ OG soubor nenulových vektorů. Uvažujme lineární kombinaci

$$\sum_{j=1}^{n} \alpha_j x_j = \theta,$$

[10] Často se používá také značení $x \perp y$.

[11] Opět užíváme Kroneckerovo delta, viz např. Kapitola 9 - Přehled použitého značení.

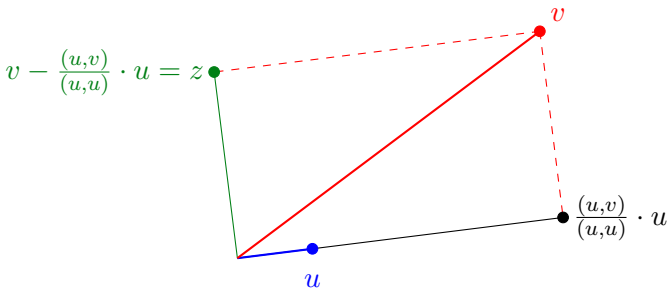
potom pro $i \in \hat{n}$ platí

$$0 = (x_i, \theta) = \left(x_i, \sum_{j=1}^{n} \alpha_j x_j \right) = \sum_{j=1}^{n} \alpha_j (x_i, x_j) = \alpha_i \|x_i\|^2,$$

kde jsme využili, že $(x_i, x_j) = 0$ pro $i \neq j$. Protože je podle předpokladu $x_i \neq \theta$, je $\|x_i\| \neq 0$ a dostáváme $\alpha_i = 0$ pro všechna $i \in \hat{n}$. Soubor vektorů $(x_1, \dots x_n)$ je proto LN. □

Dobrá tedy, každý ON soubor je tedy LN, lze ale najít ON soubor, který je dost velký, aby generoval celý prostor a byl tedy bází? Algoritmus, jak najít ON bázi v libovolném konečně dimenzionálním prehilbertově prostoru, dává důkaz následující věty, pokud jej aplikujeme na libovolnou bázi $(x_1, \dots, x_n)$.

Nejdříve si na obrázku demonstrujeme myšlenku ortogonalizace. Máme-li dva vektory u, v a chceme nahradit vektor v vektorem z tak, aby $\langle u, v \rangle = \langle u, z \rangle$ a z bylo kolmé na u.



Povšimněme si, že $\frac{(u,v)}{(u,u)} \cdot u$ je právě ta „část“ vektoru v, která je „rovnoběžná“ s u. Pokud ji od u odečteme, bude vektor $z = v - \frac{(u,v)}{(u,u)} \cdot u$ kolmý na u, přičemž tyto dva nové vektory společně generují stejný podprostor jako u a v.

Věta 8.16 (Gramova-Schmidtova ortogonalizace)**.** *Uvažujme $\mathcal{H}$ je prehilbertův prostor. Nechť $\mathcal{X} = (x_1, \dots, x_n) \subseteq \mathcal{H}$ je LN soubor vektorů, potom existuje ON soubor vektorů $\mathcal{Y} = (y_1, \dots, y_n) \subseteq \mathcal{H}$ takový, že*

$$\text{pro každé } k \in \hat{n} \text{ je } \langle x_1, \dots, x_k \rangle = \langle y_1, \dots, y_k \rangle. \tag{8.1}$$

Důkaz. Položme

$$\begin{aligned}
z_1 &= x_1\\
z_2 &= x_2 - \frac{(z_1,x_2)}{(z_1,z_1)}z_1\\
z_3 &= x_3 - \frac{(z_1,x_3)}{(z_1,z_1)}z_1 - \frac{(z_2,x_3)}{(z_2,z_2)}z_2\\
&\vdots\\
z_n &= x_n - \frac{(z_1,x_n)}{(z_1,z_1)}z_1 - \frac{(z_2,x_n)}{(z_2,z_2)}z_2 - \ldots - \frac{(z_{n-1},x_n)}{(z_{n-1},z_{n-1})}z_{n-1}.
\end{aligned} \tag{8.2}$$

[12]

Ukážeme si indukcí přes $k \in \hat{n}$, že soubor $\langle z_1,\ldots,z_k\rangle$ je OG soubor nenulových vektorů, který splňuje $\langle x_1,\ldots,x_k\rangle = \langle z_1,\ldots,z_k\rangle$.

Pro $n=1$ je zřejmé, že $z_1 = x_1$ je nenulové a $\langle z_1\rangle = \langle x_1\rangle$ a soubor (z_1) triviálně splňuje definici pro OG.

Nyní předpokládejme, že vztah platí pro $k-1$, ukážeme jeho platnost pro k. Nejdříve si rozmysleme, že $z_k \neq \theta$. Kdyby z_k bylo rovno nulovému vektoru obdrželi bychom

$$x_k \in \langle z_1,\ldots,z_{k-1}\rangle = \langle x_1,\ldots,x_{k-1}\rangle,$$

což by byl spor s lineární nezávislostí souboru $\mathcal{X}$. Díky indukčnímu předpokladu víme, že $(z_i,z_j) = 0$ pro $i,j \in \widehat{(k-1)}$. Pro OG souboru zbývá ukázat, že $(z_i,z_k) = 0$ pro $i \in \widehat{(k-1)}$:

$$\begin{aligned}
(z_i,z_k) &= \Big(z_i, x_k - \frac{(z_1,x_k)}{(z_1,z_1)}z_1 - \frac{(z_2,x_k)}{(z_2,z_2)}z_2 - \ldots - \frac{(z_{n-1},x_k)}{(z_{n-1},z_{n-1})}z_{n-1}\Big)\\
&= (z_i,x_k) - \frac{(z_1,x_k)}{(z_1,z_1)}(z_i,z_1) - \frac{(z_2,x_k)}{(z_2,z_2)}(z_i,z_2) - \ldots - \frac{(z_{n-1},x_k)}{(z_{n-1},z_{n-1})}(z_i,z_{n-1})\Big)\\
&= (z_i,x_k) - \frac{(z_i,x_k)}{(z_i,z_i)}(z_i,z_i) = 0,
\end{aligned}$$

kde využíváme toho, že $(z_i,z_j) = 0$ pro různá $i,j \in \widehat{(k-1)}$.

Ukážeme, že $\langle z_1,\ldots,z_k\rangle = \langle x_1,\ldots,x_k\rangle$. Díky předpokladu z_i pro $i \in \widehat{(k-1)}$ náleží do $\langle x_1,\ldots,x_{k-1}\rangle$ a z definice z_k plyne, že $z_k \in \langle z_1,\ldots,z_{k-1},x_k\rangle \subseteq \langle x_1,\ldots,x_{k-1},x_k\rangle$. Dohromady získáme

$$\langle z_1,\ldots,z_k\rangle \subset\subset \langle x_1,\ldots,x_k\rangle.$$

Jelikož $z_1,\ldots z_k$ jsou *OG* a nenulové, jsou z Věty 8.15, že je tento soubor LN, tudíž oba prostory mají dimenzi k a musejí se rovnat.

[12] Podobně jako v obrázku odstraňujeme z x_k části rovnoběžné s $z_1,\ldots z_{k-1}$.

Zatím je náš soubor pouze OG. Pokud toužíme po ON souboru stačí jen položit

$$y_i = \frac{1}{\|z_i\|} z_i$$

a rozmyslet si, že tyto vektory mají normu 1 a že přenásobení neovlivnilo ani jednu z požadovaných vlastností. □

Příklad 8.17. *Uvažujte $\mathbb{R}^4$ se standardním skalárním součinem. Nalezněme ON bázi podprostoru $P = \langle x_1, x_2, x_3 \rangle \subset\subset \mathbb{R}^4$, je-li*

$$x_1 = (1, 2, 2, -1), \quad x_2 = (1, 1, -5, 3), \quad x_3 = (3, 2, 8, -7).$$

Soubor (x_1, x_2, x_3) je LN, můžeme jej zortonormalizovat Gramovým Schmidtovým procesem. Jako dříve v rovnici (8.2) položíme

$$\begin{aligned}
z_1 &= x_1 = (1, 2, 2, -1) \\
z_2 &= x_2 - \frac{(z_1, x_2)}{(z_1, z_1)} z_1 = (1, 1, -5, 3) - \frac{-10}{10}(1, 2, 2, -1) = (2, 3, -3, 2) \\
z_3 &= x_3 - \frac{(z_1, x_3)}{(z_1, z_1)} z_1 - \frac{(z_2, x_3)}{(z_2, z_2)} z_2 \\
&= (3, 2, 8, -7) - \frac{30}{10}(1, 2, 2, -1) - \frac{-26}{26}(2, 3, -3, 2) = (2, -1, -1, 2).
\end{aligned}$$

Získali jsme OG soubor, který normalizujeme

$$\begin{aligned}
y_1 &= \frac{z_1}{\|z_1\|} = \frac{1}{\sqrt{10}}(1, 2, 2, -1) \quad y_2 = \frac{z_2}{\|z_2\|} = \frac{1}{\sqrt{26}}(2, 3, -3, 2) \\
y_3 &= \frac{z_3}{\|z_3\|} = \frac{1}{\sqrt{10}}(2, -1, -1, 2)
\end{aligned}$$

Soubor (y_1, y_2, y_3) je potom ON báze podprostoru P.

S ortonormální bází se velmi dobře pracuje. Zejména je velmi lehké počítat souřadnice vůči této bázi:

Věta 8.18. *Nechť $\mathcal{X} = (x_1, \ldots, x_n)$ je ON báze prehilbertova prostoru $\mathcal{H}$, potom pro každé $z \in \mathcal{H}$ platí*

$$z = \sum_{i=1}^{n} (x_i, z) x_i.$$

Neboli $(z)_{\mathcal{X}} = \big((x_1, z), (x_2, z), \ldots, (x_n, z)\big)$.

Důkaz. Jelikož $\mathcal{X}$ je báze, lze každý vektor $z \in \mathcal{H}$ napsat ve tvaru

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

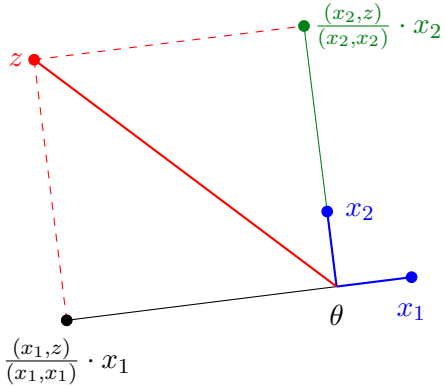
Aplikujeme tento vztah, linearitu skalárního součinu a vlastnosti ortonormální báze, obdržíme

$$(x_i, z) = (x_i, \sum_{j=1}^{n} \alpha_j x_j) = \sum_{j=1}^{n} \alpha_j (x_i, x_j) = \alpha_i, \tag{8.3}$$

kde využíváme toho, že $(x_i, x_j) = 0$ pro $i \neq j$ a $(x_i, x_j) = 1$, pokud $i = j$. □

Poznámka 8.19. *Jak je vidět z formule (8.3), pro OG bázi platí, že itá souřadnice vůči této bázi je rovna*

$$\alpha_i = \frac{(x_i, z)}{(x_i, x_i)} = \frac{(x_i, z)}{\|x_i\|^2}.$$



Obrázek 8.1: Vizualizace souřadnic vektoru z vůči bázi (x_1, x_2).

Poznámka 8.20. *Je-li $v \neq \theta$, přiřazení P_v definované jako*

$$P_v(z) := \frac{(v, z)}{(v, v)} \cdot v \text{ pro } z \in \mathcal{H}$$

se nazývá ortogonální projekce na přímku $\langle v \rangle$.

Rovnost (8.3) z Věty 8.18 lze pak přepsat do tvaru

$$z = \sum_{i=1}^{n} P_{x_i}(z) \cdot x_i.$$

8.4 Ortogonalita a symetrické matice

V této části si pro fanoušky lineární algebry konečně s pomocí dokázaných prostředků ukážeme, že v PCA a tedy i v obrázku 7.2 jsou „hlavní komponenty“ na sebe kolmé. Znalosti zde obsažené nejsou vyžadovány ke složení zkoušky, slouží pro lepší pochopení látky a jako příprava na další předměty. Dále uvažujeme pouze **standardní skalární součin nad $\mathbb{C}^n$!**

Dost často při řešení nějakého problému zjistíme, že „matice problému“ má nějaké speciální vlastnosti. Potom hlubší znalost těchto speciálních matic nám může ulehčit či umožnit nalezení řešení. Ukazuje se, že velmi důležitý atribut je symetrie.[13]

Definice 8.21. *Matice $\mathbb{A} \in T^{n,n}$ se nazývá **symetrická**, pokud*

$$\mathbb{A}^T = \mathbb{A}.^{14}$$

Začneme s tvrzením, že každá reálná symetrická matice má reálná vlastní čísla, ale nejdříve budeme potřebovat následující, pro tuto sekci klíčové lemma, které nám říká, že symetrické matice se „chovají symetricky“ vůči skalárnímu součinu.

Lemma 8.22. *Nechť $\mathbb{A} \in \mathbb{R}^{n,n}$ je symetrická matice a $x, y \in \mathbb{C}^n$, potom*

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

Důkaz. Definujme si pro $\mathbb{B} \in \mathbb{C}^{n,n}$ komplexně sdruženou matici $\overline{\mathbb{B}}$ předpisem

$$(\overline{\mathbb{B}})_{ij} = \overline{(\mathbb{B})_{ij}} \text{ pro } i, j \in \hat{n}.^{15}$$

Poctivý čtenář si snadno ale pracně ověří přímo z definice maticového násobení a komplexně sdruženého čísla platnost vztahů pro $\mathbb{B}, \mathbb{D} \in \mathbb{C}^{n,n}$

1. $\overline{\overline{\mathbb{B}}} = \mathbb{B}$,
2. $\overline{\mathbb{D} \cdot \mathbb{B}} = \overline{\mathbb{D}} \cdot \overline{\mathbb{B}}$,
3. Je-li $\mathbb{B}$ reálná matice, potom $\overline{\mathbb{B}} = \mathbb{B}$.

Konečně s využitím definice skalárního součinu a vztahu $(\mathbb{B}\mathbb{D})^T = \mathbb{D}^T\mathbb{B}^T$ obdržíme

$$(x, \mathbb{A}y) = \overline{x}^T \cdot (\mathbb{A} \cdot y) = (\mathbb{A}^T \cdot \overline{x})^T \cdot y = \overline{(\overline{\mathbb{A}^T} \cdot y)}^T \cdot y = \overline{(\mathbb{A} \cdot x)}^T \cdot y = (\mathbb{A}x, y),$$

kde využíváme $\overline{\mathbb{A}^T} = \mathbb{A}$. □

[13] Symetrická je například matice neorientovaného grafu (BI-AAG), kovarianční matice (MI-SPI), matice parciálních derivací (BI-VMM, MI-MPI).

[14] Neboli $a_{ij} = a_{ji}$ pro každé $i, j \in \hat{n}$.

[15] Prvky komplexně sdružené matice $\overline{\mathbb{B}}$ jsou tedy jsou komplexně sdružená čísla k odpovídajím prvkům původní matice $\mathbb{B}$.

Věta 8.23. *Buď $\mathbb{A} \in \mathbb{R}^{n,n}$ symetrická matice, potom*

1. *$\sigma(\mathbb{A}) \subseteq \mathbb{R}$,*
2. *vlastní vektory $\mathbb{A}$ příslušející dvěma **různým** vlastním číslům jsou vzájemně kolmé.*

Důkaz. 1. Nechť $\lambda \in \sigma(\mathbb{A})$ a $x \in \mathbb{C}^n$ příslušný vlastní vektor, tedy $x \neq \theta$ a $\mathbb{A}x = \lambda x$. Potom s pomocí Lemmatu 8.22 získáme

$$\lambda \|x\|^2 = (x, \lambda x) = (x, \mathbb{A}x) = (\mathbb{A}x, x) = (\lambda x, x) = \overline{\lambda}\|x\|^2.$$

Protože $\|x\| \neq 0$, je $\lambda = \overline{\lambda}$, odkud plyne $\lambda \in \mathbb{R}$.

2. Nechť $\lambda, \mu \in \mathbb{R}$ jsou dvě různá vlastní čísla $\mathbb{A}$ s odpovídajícími vlastními vektory x, y, tedy

$$\mathbb{A}x = \lambda x \quad \text{a} \quad \mathbb{A}y = \mu y.$$

Potom

$$\mu(x, y) = (x, \mu y) = (x, \mathbb{A}y) = (\mathbb{A}x, y) = (\lambda x, y) = \lambda(x, y),$$

odkud máme

$$(\mu - \lambda)(x, y) = 0.$$

Protože $\mu \neq \lambda$, musí platit $(x, y) = 0$.

□

Pozorování 8.24. *Má-li matice $\mathbb{A} \in \mathbb{R}^{n,n}$ reálné vlastní číslo, pak lze jeho vlastní vektory zvolit reálné.*

Přesněji: Je-li $\mathbb{A} \in \mathbb{R}^{n,n}$ a $\lambda_0 \in \sigma(\mathbb{A})$, $\lambda_0 \in \mathbb{R}$, potom existuje báze vlastního podprostoru příslušejícího λ_0 [16]*, která je složena z vektorů náležících $\mathbb{R}^n$.*

Důkaz. Soustava $(\mathbb{A} - \lambda_0\mathbb{E}|\theta)$ obsahuje pouze reálná čísla. Algoritmus GEMu 1.32 používá pouze (G1) a (G3), kde odečítáme reálné násobky reálného prvního řádku. Tyto kroky zachovají všechny řádky reálné, tedy jeho aplikací získáme soustavu v HST, která má všechny prvky reálné.

Zbývá si jen uvědomit, že pokud zvolíme do příslušných volných proměnných reálnou bázi[17], vázané proměnné pak budou také reálné. □

Následuje tvrzení o tom, že každá reálná symetrická matice je diagonalizovatelná.

[16] To jest báze řešení homogenní soustavy $(\mathbb{A} - \lambda_0\mathbb{E}|\theta)$.

[17] Třeba standardní bázi.

Věta 8.25. *Nechť $\mathbb{A} \in \mathbb{R}^{n,n}$ je symetrická matice, potom pro každé vlastní číslo $\lambda_0 \in \sigma(\mathbb{A})$ je $\nu_g(\lambda_0) = \nu_a(\lambda_0)$.*

Důkaz. Nechť pro spor platí $k := \nu_g(\lambda_0) < \nu_a(\lambda_0)$. Z definice geometrické násobnosti potom existuje kčlenná báze vlastního podprostoru příslušející vlastnímu číslu λ_0 (tj. řešení soustavy $(\mathbb{A} - \lambda_0\mathbb{E}|\theta)$), označme si ji $(x_1, \dots x_k)$. Doplníme tento soubor na $(x_1, \dots x_n)$ tak, aby tvořil bázi celého $\mathbb{C}^n$.

Díky Gramově-Schmidtově ortogonalizaci (Věta 8.16) ji nahradíme za ON bázi $\mathcal{Y} := (y_1, \dots, y_n)$, která splňuje $\langle y_1, \dots, y_k\rangle = \langle x_1, \dots, x_k\rangle$. Tedy $y_1, \dots, y_k$ je ON báze vlastního podprostoru příslušející λ_0, speciálně jsou to tedy vlastní vektory patřící λ_0.

S pomocí Lemmatu 8.22 si povšimneme, že vektory $\mathbb{A}y_j$ jsou kolmé na y_i pro $i \in \{1, \dots k\}$, $j \in \{k+1, \dots n\}$:

$$(y_i, \mathbb{A}y_j) = (\mathbb{A}y_i, y_j) = (\lambda_0 y_i, y_j) = \lambda_0(y_i, y_j) = 0. \tag{8.4}$$

Jako dříve uvažujme o $\mathbb{A}$ jako o zobrazení $A(x) := \mathbb{A} \cdot x$. Pro $i \in \hat{k}$ jsou y_i vlastní vektory k λ_0, proto $(Ay_i)_{\mathcal{Y}} = (\lambda_0 y_i)_{\mathcal{Y}} = \lambda_0 e_i$. Z Věty 8.18 a vztahu (8.4) víme, že prvních k souřadnic Ay_j vůči bázi $\mathcal{Y}$ je rovno 0.

Proto má matice zobrazení A vzhledem k bázi $\mathcal{Y}$ tvar

$${}^{\mathcal{Y}}A = \begin{pmatrix} \lambda_0\mathbb{E}_k & \Theta_{k,n-k} \\ \Theta_{n-k,k} & \mathbb{B} \end{pmatrix} \in \mathbb{C}^{n,n},$$

kde $\mathbb{B}$ je nějaká matice z $\mathbb{C}^{n-k,n-k}$.

Jelikož $\mathbb{A}$ i A mají stejné spektrum včetně násobností, obdržíme

$$p_{\mathbb{A}}(\lambda) = p_A(\lambda) = \det {}^{\mathcal{Y}}(A - \lambda E) = \begin{pmatrix} (\lambda_0 - \lambda)\mathbb{E}_k & \Theta_{k,n-k} \\ \Theta_{n-k,k} & \mathbb{B} - \lambda\mathbb{E}_{n-k} \end{pmatrix}.$$

Rozvojem determinantu podle prvních k sloupců obdržíme, že

$$p_{\mathbb{A}}(\lambda) = (\lambda_0 - \lambda)^k \, p_{\mathbb{B}}(\lambda).$$

Z předpokladu je násobnost λ_0 v $p_{\mathbb{A}}(\lambda)$ větší než k, tudíž λ_0 musí být kořenem $p_{\mathbb{B}}(\lambda)$. Tedy λ_0 je vlastním číslem $\mathbb{B}$ a existuje vlastní vektor $u = (u_{k+1}, \dots, u_n) \in \mathbb{C}^{n-k}$, tak že $u \neq \theta$ a $\mathbb{B}u = \lambda_0 u$.

Položme

$$x = \sum_{j=k+1}^{n} u_j y_j$$

potom

$$x \notin \langle y_1, \dots, y_k\rangle \text{ a } (x)_{\mathcal{Y}} = (0, \dots, 0, u_{k+1}, \dots, u_n).$$

Z Věty 5.27 a vlastnosti maticového násobení obdržíme

$$(Ax)_{\mathcal{Y}} = {}^{\mathcal{Y}}A \cdot (x)_{\mathcal{Y}} = \sum_{i=1}^{n} ((x)_{\mathcal{Y}})_i \mathbb{A}_{:i} = \sum_{i=k+1}^{n} u_i \mathbb{A}_{:i}$$
$$= \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \mathbb{B} \cdot u \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \lambda_0 u \end{pmatrix} = (\lambda_0 x)_{\mathcal{Y}},$$

Proto platí $\mathbb{A}x = Ax = \lambda_0 x$. Neboli x je další vlastní vektor přišlušející λ_0, což je spor s tím, že geometrická násobnost λ_0 je k. □

Už teda víme, že pro reálnou symetrickou matici existuje báze $\mathbb{C}^n$ složená z jejích vlastních vektorů. Platí dokonce silnější tvrzení. Tato báze může být navíc zvolena ON!

Věta 8.26. *Nechť $\mathbb{A} \in \mathbb{R}^{n.n}$ je symetrická. Potom existují vlastní vektory $y_1, \dots y_n$ takové, že soubor $(y_1, \dots, y_n)$ je ON báze $\mathbb{C}^n$.*

Důkaz. Nechť $\mathbb{A}$ má různé vlastní čísla $\lambda_1, \dots, \lambda_k$. Nalezneme bázi vlastního podprostoru příslušející vlastnímu číslu λ_i s geometrickou násobností l_i. Díky Gramově-Schmidtově ortogonalizaci (Věta 8.16) můžeme předpokládat, že tato báze podprostoru je ON. Označmě si ji $(x_1^i, \dots, x_{l_i}^i)$. Naše hledaná ON báze bude

$$(x_1^1, \dots, x_{l_1}^1, \dots, x_1^k, \dots, x_{l_k}^k).$$

Díky předchozí větě víme, že tento soubor obsahuje n vektorů. Z konstrukce je zřejmé, že

$$(x_j^i, x_j^i) = 1 \text{ a } (x_j^i, x_m^i) = 0 \text{ pro } i \in \hat{k},\ j, m \in \hat{l}_i.$$

Jelikož u_j^i a u_m^t jsou vlastní vektory příslušející různým vlastním číslům obdržíme z Věty 8.23:

$$(x_j^i, x_m^t) = 0 \text{ pro } i, t \in \hat{k},\ j, m \in \hat{l}_i.$$

Dohromady jsme ověřili, že tento soubor je ortonormální □

Pozorování 8.27. *Je-li $\mathcal{X} = (x_1, \dots, x_n)$ ON báze $\mathbb{C}^n$ potom*

$$\overline{({}^{\mathcal{X}}E^{\mathcal{E}})}^T \cdot {}^{\mathcal{X}}E^{\mathcal{E}} = \mathbb{E}.$$

Neboli

$$({}^{\mathcal{X}}E^{\mathcal{E}})^{-1} = {}^{\mathcal{E}}E^{\mathcal{X}} = \overline{({}^{\mathcal{X}}E^{\mathcal{E}})}^T.$$[18]

Speciálně, pokud jsou $x_1, \dots, x_n$ reálné vektory máme

$$({}^{\mathcal{X}}E^{\mathcal{E}})^{-1} = {}^{\mathcal{E}}E^{\mathcal{X}} = ({}^{\mathcal{X}}E^{\mathcal{E}})^T.$$[19]

[18] Maticím, které splňují $\mathbb{A}^{-1} = \overline{\mathbb{A}}^T$, se říká **unitární** matice.
[19] Maticím, které splňují $\mathbb{A}^{-1} = \mathbb{A}^T$, se říká **ortogonální** matice.

Pokud dáme všechny předchozí části dohromady, finálně dostaneme, že reálná symetrická matice je „hezky“ diagonizovatelná.

Důsledek 8.28 (Spektrální věta)**.** *Buď $\mathbb{A} \in \mathbb{R}^{n,n}$ reálná symetrická matice. Potom je $\mathbb{A}$ podobná diagonální matici $\mathbb{D} \in \mathbb{R}^{n,n}$, navíc regulární matici $\mathbb{P} \in \mathbb{R}^{n,n}$ z relace podobnosti lze volit takovou, že $\mathbb{P}^{-1} = \mathbb{P}^T$. Tedy platí*

$$\mathbb{A} = \mathbb{P}^T \mathbb{D} \mathbb{P}.$$

Důkaz. Z Věty 8.23 víme, že vlastní čísla jsou reálná, díky Pozorování 8.24 můžeme volit i vlastní vektory reálné. Díky důkazu Věty 8.26 víme, že lze volit vlastní vektory ON.

V důkazu se užila Gram-Schmidtova ortogonalizace. Povšimněme si, že pokud byly původní vektory reálné, potom budou po ortonormalizaci i výsledné vektory budou reálné. Proto existuje ON báze vlastních vektorů, nazveme ji $\mathcal{X}$.

Uvažujme zobrazení $A(x) = \mathbb{A} \cdot x$. Potom obdržíme

$$\mathbb{A} = {}^{\mathcal{E}}A = {}^{\mathcal{X}}E^{\mathcal{E}} \,.\, {}^{\mathcal{X}}A \,.\, {}^{\mathcal{E}}E^{\mathcal{X}}.$$

Nyní stačí položit $\mathbb{D} = {}^{\mathcal{X}}A$ a $\mathbb{P} = {}^{\mathcal{E}}E^{\mathcal{X}}$.[20] Díky Pozorování 8.27 získáme, že

$$\mathbb{P}^T = ({}^{\mathcal{E}}E^{\mathcal{X}})^T = \left(({}^{\mathcal{X}}E^{\mathcal{E}})^T\right)^T = {}^{\mathcal{X}}E^{\mathcal{E}}.$$

□

Poznámka 8.29. *V celé této části jsme potřebovali jen Lemma 8.22, kde jsme v důkazu potřebovali pouze, že*

$$\overline{\mathbb{A}^T} = \mathbb{A}$$

*Maticím, které splňují tento vztah, se říká **hermitovské** či také samosdružené matice.*

Vašnivý čtenář si snadno ověří, že ve všech větách v této části, lze předpoklad „$\mathbb{A} \in \mathbb{R}^{n,n}$ je symetrická matice“ nahradit za obecnější „$\mathbb{A} \in \mathbb{C}^{n,n}$ je hermitovská matice“ a získat analogie předchozích vět.

[20] Rozmyslete si, že $\mathbb{D}$ je diagonální matice, která obsahuje na diagonále vlastní čísla.

Kapitola 9

Přehled použitého značení

V této části přidáváme pro lepší orientaci v textu přehled použitého značení, včetně jeho prvního výskytu. Číslo XX znamená, že byl poprvé užit na straně XX. Zkratkou dXX myslíme, že symbol byl užit v definici, která začíná na straně XX (a symbol se může vyskytovat na další stránce, pokud byla definice moc dlouhá).

symbol	zaveden	význam
$:=$		definice, symbol na levé straně je definován výrazem na pravé straně
$\emptyset$		množina prázdná
A, B, C, M, N		množiny
$A, B \in \mathcal{L}(P, Q)$	d157	lineární zobrazení z P do Q
$\#A$		počet prvků v množině A
$\min A$		nejmenší prvek v množině A
$A \subseteq B$		A je podmnožinou B
$A \subsetneq B$		A je vlastní podmnožinou B, tj $A \subseteq B$ a $A \neq B$
$A + B$	d22	součet množin A a B
	180	součet zobrazení A a B
αA	d22	αnásobek množiny A
	180	αnásobek zobrazení A
$A \oplus B$	d78	direktní součet množin A a B
$a + A$	d22	součet čísla/vektoru a a množiny A
Ax	158	obraz vektoru x
A^{-1}		inverzní zobrazení k A
AB	158	složení zobrazení A a B
$d(A)$	d165	defekt zobrazení A
$h(A)$	d165	hodnost zobrazení A
$\ker A$	d165	jádro zobrazení A

${}^{\mathcal{X}}A$	d177	matice zobrazení A vzhledem k $\mathcal{X}$, $\mathcal{X}$, tj. ${}^{\mathcal{X}}A^{\mathcal{X}}$
${}^{\mathcal{X}}A^{\mathcal{Y}}$	d177	matice zobrazení A vzhledem k $\mathcal{X}$, $\mathcal{Y}$
E	d157	identický operátor
${}^{\mathcal{X}}E^{\mathcal{Y}}$	d183	matice přechodu od báze $\mathcal{X}$ k bázi $\mathcal{Y}$
G_K	d124	generující matice kódu
H_K	d124	kontrolní matice kódu
K	d124	kód
$\mu(K)$	d127	minimální vzdálenost kódu
$\langle M \rangle$	d62	lineární obal množiny vektorů
S	d20	řešení soustavy $\mathbb{A}\mathbb{x} = \mathbb{b}$
S_0	d20	řešení homogenní soustavy $\mathbb{A}\mathbb{x} = \theta$
S_n	d204	permutace množiny $\{1, \dots, n\}$
V, P, Q	d47	vektorový prostor
$P \subset\subset V$	d53	P je podprostor V
V_n, P_n, Q_n	d81	vektorový prostor dimenze $n \in \mathbb{N}$
$\dim V$	d71	dimenze vektorového prostoru V
W	d110	varieta
$Z(W)$	d110	zaměření variety
$\dim W$	d110	dimenze variety
HST	28	horní stupňovitý tvar
GEM	32	Gaussova eliminace
LZ	d58, d62	lineárně závislý
LN	d58, d62	lineárně nezávislý
OG	d267	ortogonální
ON	d267	ortonormální
VP	48	vektorový prostor
$\mathbb{N}$		množina přirozených čísel $\mathbb{N} = \{1, 2, \dots\}$
$\mathbb{Z}$		množina celých čísel
$\mathbb{Z}_n$	37	množina $\{0, \dots, n-1\}$ vybavená operacemi $+_n, \cdot_n$
$\mathbb{Q}$		těleso racionálních čísel
$\mathbb{R}$		těleso reálných čísel
$\mathbb{R}^+$		množina $(0, \infty)$
$\mathbb{R}^m$	d20	$m$tice reálných čísel, ztotožňujeme s jednorozměrnou maticí $\mathbb{R}^{m,1}$
$\mathbb{R}^{m,n}$	d14	reálná matice s m řádky a n sloupci
$\mathbb{C}$		těleso komplexních čísel
T	d40	těleso
T^m	41	$m$tice čísel z tělesa T, ztotožňujeme s jednorozměrnou maticí $T^{m,1}$
$T^{m,n}$	41	matice s m řádky a n sloupci, jejíž prvky patří do tělesa T
$\mathbb{A}, \mathbb{B}, \mathbb{D}, \mathbb{P}, \mathbb{X}, \mathbb{Y}$	d14	matice

$\mathbb{A}_{i:}$	d14	$i$tý řádek matice
$\mathbb{A}_{:j}$	d14	$j$tý sloupec matice
$\alpha\mathbb{A}$	d14	αnásobek matice $\mathbb{A}$
$\mathbb{A}+\mathbb{B}$	d14	součet matic $\mathbb{A}$ a $\mathbb{B}$
$\mathbb{A}^T$	d16	transpozice matice $\mathbb{A}$
$\mathbb{A}^{-1}$	d92	inverzní matice k matici $\mathbb{A}$
$\overline{\mathbb{A}}$	272	sdružená matice k matici $\mathbb{A}$
$\mathbb{A}\mathbb{B}$	d16	součin matice $\mathbb{A}$ a $\mathbb{B}$
$\alpha\mathbb{A}$	d14	αnásobek matice $\mathbb{A}$
$\operatorname{adj}\mathbb{A}$	d224	adjungovaná matice k matici $\mathbb{A}$
$\det\mathbb{A}, \lvert\mathbb{A}\rvert$	d209	determinant matice $\mathbb{A}$
$h(\mathbb{A})$	d86	hodnost matice
$\mathbb{A}(k,\ell)$	d221	matice vzniklá z $\mathbb{A}$ vynecháním $k$tého řádku a ℓtého sloupce
$\mathbb{A}\sim\mathbb{B}$	d86	$\mathbb{A}$ lze převést pomocí GEM na $\mathbb{B}$
$(\mathbb{A}\mid\mathbb{b})$	d20	matice soustavy $\mathbb{A}\mathbb{x}=\mathbb{b}$
$\mathbb{b}$	d20	vektor T^n, nejčastěji vektor pravých stran
$\mathbb{E}, \mathbb{E}_n$	d92	jednotková matice, jednotková matice z $T^{n,n}$
$\mathbb{x}$	d20	vektor, nejčastěji vektor neznámých
$\sum_{i=1}^{n} x_i$		součet prvků $x_1, x_2 \ldots x_n = x_1 + x_2 + \cdots + x_n$
$\Pi_{i=1}^{n} x_i$		součin prvků $x_1, x_2 \ldots x_n = x_1 \cdot x_2 \cdot \cdots \cdot x_n$
Θ	d20	nulová matice v $T^{m,n}$, tzn. všechny její prvky jsou rovny nule
(n,k)-kód	d58, d132	lineární (n,k)-kód
α, β, γ	49	skaláry, tj. prvky z tělesa T
δ	d140, d143	dekódování
δ_{ij}	92	Kroneckerovo delta
κ	d124	kódování
λ	d230, d239	vlastní číslo
$\nu_a(\lambda)$	d235, d240	algebraická násobnost vlastního čísla λ
$\nu_g(\lambda)$	d232, d240	geometrická násobnost vlastního čísla λ
π_u	d143	pivot slova u
π, σ, τ	d204	permutace
$\operatorname{sgn}\pi$	d206	znaménko permutace π
$\sigma(A)$	d230	spektrum operátoru A
$\sigma(\mathbb{A})$	d239	spektrum matice $\mathbb{A}$
τ_{ij}	d207	transpozice čísel i a j
θ	d47	nulový vektor
$\theta\in\mathbb{R}^n$	d20	$\theta=(0,\ldots,0)$
θ_P	161	nulový vektor prostoru P
$a, b, c, \ldots x, y, z$	49	vektory
f, g, h		zobrazení

i, j, k, l, m, n		nejčastěji přirozená/celá čísla
$\hat{n}$	d27	množina $\{1, \ldots, n\}$
s, t		nejčastěji reálná čísla
x, y, z, u, v		také složky vektoru $(x, y, z) \in \mathbb{R}^3$, resp $(x, y, z, u, v) \in \mathbb{R}^5$
$\overline{z}$		komplexně sdružené číslo, $\overline{a + bi} = a - bi$
$\operatorname{Re} z$		reálná část komplexního čísla, $\operatorname{Re} a + bi = a$
$\operatorname{Im} z$		imaginární část komplexního čísla, $\operatorname{Im} a + bi = b$
$f(M)$	156	obraz množiny M při zobrazení f
$f^{-1}(y)$	156	vzor prvku y při zobrazení f
$f^{-1}(M)$	156	vzor množiny N při zobrazení f
$p_A(\lambda)$	233, d234	charakteristický polynom operátoru A
$p_{\mathbb{A}}(\lambda)$	d239	charakteristický polynom matice $\mathbb{A}$
$(x_1, \ldots, x_n) \in T^n$	58	vektor z T^n se souřadnicemi $x_1, \ldots, x_n$
$(x_1, \ldots, x_n) \subseteq V$	57	soubor vektorů z V délky n
$(x, y) \in T$	d8.1	skalární součin vektorů z $\mathcal{H}$
$\langle x_1, \ldots, x_n \rangle$	d62	lineární obal souboru vektorů
$(z)_{\mathcal{X}}$	d82	souřadnice vektoru vůči bázi $\mathcal{X}$
$(.)_{\mathcal{X}}$	159	souřadnicový izomorfismus
$x_i^{\#}(z)$	d82	$i$tá souřadnice vektoru vůči bázi $\mathcal{X}$
$x_i^{\#}$	159	$i$tý souřadnicový funkcionál
$d(u, v)$	d126	Hammingova vzdálenost slov u, v
$\|u\|$	d138	Hammingova váha slova u
$\|u\|$	d264	norma vektoru u
$\mathcal{A}$	d121	abeceda
$\mathcal{A}^n$	d121	množina slov délky n nad abecedou $\mathcal{A}$
$\mathcal{B}$		v Kap. 4 abeceda, jinak báze
$\mathcal{E}, \mathcal{E}_n$	62	standardní báze T^n
$\mathcal{E}_{m,n}$	70	standardní báze matic $T^{m,n}$
$\mathcal{H}$	263	prehilbertův prostor
$\mathcal{L}(P, Q)$	d157	množina lineárních zobrazení z P do Q
$\mathcal{L}(V)$	d157	množina operátorů na V
$\mathcal{X}, \mathcal{Y}, \mathcal{Z}$		soubor vektorů

Rejstřík

úhel, 266
řádek matice, 14
řešení, 9
    množina řešení, 21
        homogenní soustavy, 21
    partikulární, 100

abeceda, 121
algebraická násobnost, 235, 240

báze, 68
    standardní, 71
bod, 111

charakteristický polynom
    matice, 239
    operátoru, 234
chyba
    objevování chyb, 127
    opravování chyb, 128

defekt zobrazení, 165
dekódování, 140
    standardní, 143
determinant, 209
diagonála, 92
dimenze
    variety, 110
    vektorového prostoru, 71

funkcionál, 157
    souřadnicový, 82, 159

Gaussova eliminace (GEM), 30, 32
geometrická násobnost, 232, 240
Gramova-Schmidtova ortogonalizace, 268
grupa, 39
    Abelova, 39

hodnost
    matice, 86
    zobrazení, 165
horní stupňovitý tvar, 28
hyperkrychle, 145

inverze v permutaci, 206
izomorfismus, 158
    souřadnicový, 159

jádro zobrazení, 165

kód, 124
    (n, k)-kód, 132
    binární, 145
    binární Hammingův, 146
    koktavý, 130
    lineární, 132
    MDS, 152
    opakovací, 122
    paritní, 125
    systematický, 131
kódování, 124
kodimenze variety, 110
Kroneckerovo delta, 92

lemma
    Steinitzovo, 73

lineární kombinace, 58
    triviální, 58
lineární obal
    množiny, 62
    souboru, 62
lineárně nezávislá/ý (LN)
    množina, 62
    soubor vektorů, 58
lineárně závislá/ý (LZ)
    množina, 62
    soubor vektorů, 58

matice, 14
    čtvercová, 17
    adjungovaná, 224
    determinant, 209
    diagonála, 92
    diagonální, 92
    diagonizovatelná, 247
    generující, 132
    hodnost, 86
    horní trojúhelníková, 25
    inverzní, 92
    jednotková, 92
    kontrolní, 132
    nulová, 20
    přechodu, 183
    podobné, 243
    regulární, 92
    rozšířená, 20
    singulární, 92
    soustavy, 20
    symetrická, 272
    transpozice, 16
    zobrazení, 177
množina
    lineárně závislá (LN), 62
    lineárně závislá (LZ), 62

násobení
    čísla a množiny, 22
    modulo, 37

nadrovina, 112
neparametrické rovnice, 114
nerovnost
    Schwarzova, 265
    trojúhelníková, 265
norma, 264

operátor, 157
    charakteristický polynom, 234
    diagonizovatelný, 247
    identický, 157
    spektrum operátoru, 231

přímka, 111
parametrické rovnice, 114
permutace, 204
    inverze v permutaci, 206
    znaménko, 206
pivot, 141, 143
podprostor, 53
    triviální, 54
    vlastní, 54
    vlastní příslušející vlastnímu číslu, 232
prehilbertův prostor, 263
proměnná
    vázaná, 103
    volná, 103
prvek
    inverzní, 39
    jednotkový, 40
    neutrální, 39
    nulový, 40

rovina, 112

skalár, 48
skalární součin, 263
    standardní, 264
sloupec
    hlavní, 28
    matice, 14
    vedlejší, 28

slovo
kódové, 124
součet
direktní, 78
množin, 22
modulo, 37
souřadnice vektoru, 82
souřadnicový funkcionál, 82
soubor vektorů, 57
generuje, 68
lineárně nezávislý (LN), 58
lineárně závislý (LZ), 58
ortogonální, 267
ortonormální, 267
soustava rovnic
homogenní, 9, 20
maticový zápis, 20
nehomogenní, 9, 30
přidružená homogenní, 20
spektrum, 231
matice, 239
syndrom, 144

těleso, 41
tabulka
dekódovací, 143
syndromová, 144
transpozice
čísel, 207
matice, 16

váha
Hammingova, 138
věta
1. o dimenzi, 79
2. o dimenzi, 168
Frobeniova, 100
Pythagorova, 267
Singletonův odhad, 131
varieta, 110
dimenze, 110
kodimenze, 110
neparametrické rovnice, 114
parametrické rovnice, 114
zaměření, 110
vektor, 48
úhel vektorů, 266
norma vektoru, 264
nulový v $\mathbb{R}^n$, 20
v $\mathbb{R}^n$, 20
neznámých, 20
nulový, 48
opačný, 49
posunutí, 110
pravých stran, 20
směrový, 110
souřadnice vektoru, 82
soubor vektorů, 57
vektorový prostor, 47
vlastní číslo, 230
algebraická násobnost, 235, 240
geometrická násobnost, 232, 240
matice, 239
vlastní vektor, 231
matice, 239
vzdálenost
Hammingova, 126
minimální kódu, 127

zaměření variety, 110
znak
informační, 130
kontrolní, 130
zobrazení, 156
bijektivní, 157
defekt, 165
hodnost, 165
identické, 157
injektivní, 157
inverzní, 157
jádro, 165
lineární, 157
na, 157
prosté, 157

složené, 157
surjektivní, 157