Petr Olšák

Lineární algebra

Praha, druhé vydání 2010

Text ve formátech TEX (csplain), PostScript, dvi, PDF najdete na adrese
ftp://math.feld.cvut.cz/pub/olsak/linal/.

Verze textu: 21. 6. 2017 (beta verze druhého vydání)

Upozornění: Tento dokument je v rozpracovaném stavu. Bude se ještě během roku 2010 výrazně měnit.

Text vznikal postupně od roku 2000 a je od té doby volně šířen na uvedených stránkách. Nové partie jsem až do roku 2007 připojoval na konce stávajících kapitol, abych neporušil číslování již existujících odstavců. V červnu 2007 jsem tento text použil ve skriptech [20]. Tam je navíc ke každé kapitole připojena rozsáhlá sbírka cvičení a je přidána kapitola o polynomech. Tyto věci ve verzi volně šířené na internetu nejsou.

V roce 2010 jsem začal pracovat na „druhém vydání“ tohoto textu, který se výrazně liší od předchozího. V některých partiích jsem začal používat (domnívám se) užitečnější značení, ale především jsem text rozčlenil do kapitol výrazně jiným způsobem a opustil jsem od zpětné kompatibility číslování odstavců s první verzí. Druhé vydání má zdrojový soubor `linal2.tex`. K teoretickému úvodu (lineární prostor, lineární závislost, obaly, báze) přidávám pojem souřadnice vzhledem k bázi a v následující kapitole o zobrazeních ukážu, že souřadnice vzhledem k bázi jsou izomorfismem na $\mathbf{R}^n$. Tím vytvořím motivaci podrobněji studovat vlastnosti v $\mathbf{R}^n$ včetně popisu algoritmů. Takže až poté přicházejí na řadu kapitoly o maticích. K lineárním zobrazením se pak vracím podruhé, abych uvedl jejich souvislost s maticemi.

V druhém vydání jsem zcela přepracoval kapitoly o lineárních zobrazeních a dále jsem přidal mnoho dalších partií, které souvisejí s praktickými aplikacemi: vyšetřování lineárních obalů, LU rozklad, blokový maticový součin, Strassenův algoritmus, geometrická interpretace množiny řešení soustavy rovnic, matice afinního zobrazení v homogenních souřadnicích. Na konec každé kapitoly jsem připojil odstavec „shrnutí“, který lapidárním jazykem shrnuje, co bylo v kapitole řečeno.

Některé odstavce jsem nově označil hvězdičkou. Tím je řečeno, že odstavec obsahuje důležitý výsledek lineární algebry, který rozhodně stojí za povšimnutí. To umožní čtenáři se rychleji orientovat v tom, které partie textu obsahují skutečně zásadní informace a určitě by je neměl přeskočit.

Obsah

Gaussova eliminační metoda

Než se pustíme do studia lineárních prostorů a podprostorů, závislosti a nezávislosti vektorů, bází a lineárních obalů, uvedeme si v této úvodní kapitole metodu, která se nám bude často hodit. Protože se k řešení soustav vrátíme podrobněji v kapitole ??, řekneme si zde jen to nejnutnější a budeme se v některých případech vyjadřovat možná poněkud těžkopádně. Vše napravíme v ?? kapitole.

Gaussova eliminační metoda je metoda usnadňující řešení soustav lineárních rovnic. *Soustava lineárních rovnic* je jedna nebo (obvykle) více lineárních rovnic, které mají být splněny všechny současně. *Lineární rovnice* je rovnice, ve které se jedna nebo (obvykle) více neznámých vyskytuje pouze v první mocnině. Neznámé mohou být násobené různými konstantami a tyto násobky se v součtu mají rovnat dané konstantě, tzv. *pravé straně*. *Řešit soustavu rovnic* znamená najít řešení, tj. najít taková reálná čísla, která po dosazení za neznámé v rovnicích splňují všechny rovnice současně. Takové řešení může existovat pro danou soustavu jediné, může se ale stát, že je takových řešení více nebo není žádné.

Metodu si nejprve vysvětlíme na jednoduchém příkladě následující soustavy dvou lineárních rovnic o dvou neznámých x, y:

$$\begin{aligned} 2x - 5y &= 16 \\ -x + 2y &= -7 \end{aligned}$$

Ze střední školy asi znáte dvě metody, jak takové soustavy řešit: buď postupným dosazením, nebo násobením rovnic konstantami a vzájemným sčítáním rovnic. Metoda postupného dosazení by mohla vypadat takto:

$$\begin{array}{l} 2x-5y=\ \ 16 \\ -x+2y=-7 \ \Rightarrow\ \ x=2y+7 \end{array} \Rightarrow\ 2(2y+7)-5y=14-y=16\ \Rightarrow\ \underline{y=-2} \Rightarrow\ x=2(-2)$$

ale nemá s Gaussovou eliminační metodou moc společného. Pro rozsáhlejší soustavy (mnoho rovnic, mnoho neznámých) se moc nehodí. Zaměříme se proto na druhou metodu „sčítání rovnic“. V této metodě měníme postupně soustavu rovnic na jinou soustavu se stejným řešením. Změny soustavy, které nemění řešení, jsou následující:

(1) Prohození rovnic mezi sebou.
(2) Vynásobení rovnice nenulovou konstantou.
(3) Přičtení libovolného násobku nějaké rovnice k jiné.

Pomocí těchto úprav převedeme soustavu rovnic na jinou soustavu, ze které je již řešení snadno čitelné. Jednotlivé modifikace naší soustavy od sebe oddělujeme znakem „$\sim$“.

$$\begin{array}{r} 2x-5y=\ \ 16 \\ -x+2y=-7 \end{array} \sim \begin{array}{r} 2x-5y=\ \ 16 \\ -2x+4y=-14 \end{array} \sim \begin{array}{r} 2x-5y=16 \\ 0x-\ \ y=\ \ 2 \end{array} \sim\sim \begin{array}{r} 2x-5y=\ \ 16 \\ y=-2 \end{array} \sim \begin{array}{r} 2x+0y=\ \ 6 \\ y=-2 \end{array}$$

Nejprve jsme vynásobili druhou rovnici dvěma, pak jsme obě rovnice sečetli a výsledek napsali na místo druhé rovnice, dále jsme druhou rovnici vynásobili číslem -1, pak jsme pětinásobek

druhé rovnice přičetli k první a nakonec jsme první rovnici vynásobili číslem $1/2$. Z poslední soustavy čteme přímo řešení.

Gaussova eliminační metoda je vlastně shodná s právě použitou metodou „sčítání rovnic“. Navíc Gaussova metoda upřesňuje postup, jak rovnice násobit a sčítat mezi sebou, abychom se cíleně dobrali k výsledku i u rozsáhlých soustav mnoha rovnic s mnoha neznámými. Než tento postup popíšeme, zamyslíme se nad tím, jak stručně můžeme soustavy rovnic zapisovat. V soustavě rovnic není při hledání řešení podstatné, zda se neznámé jmenují x, y, z nebo třeba α, β, γ. Podstatné jsou jen koeficienty, které násobí jednotlivé neznámé, a samozřejmě ještě hodnoty na pravých stranách rovnic. Oddělíme tedy „zrno od plev“ a vypíšeme z naší soustavy jen to podstatné (koeficienty u neznámých a hodnoty pravých stran) do tabulky čísel, které budeme říkat *matice*:

$$\left(\begin{array}{rr|r} 2 & -5 & 16 \\ -1 & 2 & -7 \end{array}\right)$$

Pokud chceme prohodit rovnice, v novém značení to znamená prohodit řádky matice. Vynásobení rovnice nenulovou konstantou odpovídá vynásobení řádku matice touto konstantou. Konečně přičtení násobku jedné rovnice k druhé je totožné s přičtením násobku jednoho řádku ke druhému. Postup řešení našeho příkladu tedy můžeme zapsat takto:

$$\left(\begin{array}{rr|r} 2 & -5 & 16 \\ -1 & 2 & -7 \end{array}\right) \sim \left(\begin{array}{rr|r} 2 & -5 & 16 \\ -2 & 4 & -14 \end{array}\right) \sim \left(\begin{array}{rr|r} 2 & -5 & 16 \\ 0 & -1 & 2 \end{array}\right) \sim \left(\begin{array}{rr|r} 2 & -5 & 16 \\ 0 & 1 & -2 \end{array}\right) \sim \left(\begin{array}{rr|r} 2 & 0 & 6 \\ 0 & 1 & -2 \end{array}\right) \sim \left(\begin{array}{rr|r} 1 & \\ 0 & \end{array}\right.$$

Před výkladem Gaussovy eliminační metody na obecné soustavě lineárních rovnic si ukážeme postup ještě na jednom příkladu, který bude mít čtyři rovnice a pět neznámých. Příklad je zvolen záměrně tak, aby vycházela malá celá čísla, takže se nám to bude dobře počítat bez použití výpočetní techniky. To je obvyklé v tzv. *modelových příkladech*, které mají za úkol ilustrovat obecné algebraické postupy a se kterými se setkáte při řešení úloh ze skript. Jakmile se ale dostanete k úlohám z praxe, budete postaveni před soustavy třeba s tisíci rovnicemi a se zhruba stejným počtem neznámých. Na malá celá čísla budete muset zapomenout. Bez výpočetní techniky se to pak řešit nedá. Pamatujte tedy, že řešení modelových příkladů ze skript není konečným cílem naší teorie, ale jen pomůckou k pochopení rozsáhlejších souvislostí.

Máme řešit následující soustavu lineárních rovnic

$$\begin{array}{rcrcrcrcr}
-4x_1 & + & 4x_2 & - & x_3 & + & x_4 & - & 7x_5 & = & -11 \\
2x_1 & - & 2x_2 & + & x_3 & & & + & 3x_5 & = & 4 \\
4x_1 & - & 4x_2 & + & 5x_3 & + & x_4 & + & 7x_5 & = & -3 \\
-6x_1 & + & 6x_2 & - & 4x_3 & + & x_4 & - & 12x_5 & = & -7
\end{array}$$

Koeficienty této soustavy přepíšeme do matice a matici budeme upravovat pomocí tzv. kroků Gaussovy eliminační metody, mezi které patří prohození řádků mezi sebou, vynásobení řádku nenulovou konstantou nebo přičtení libovolného násobku nějakého řádku k jinému.

$$\left(\begin{array}{rrrrr|r} -4 & 4 & -1 & 1 & -7 & -11 \\ 2 & -2 & 1 & 0 & 3 & 4 \\ 4 & -4 & 5 & 1 & 7 & -3 \\ -6 & 6 & -4 & 1 & -12 & -7 \end{array}\right) \sim$$

Nejprve potřebujeme sčítáním násobků řádků dostat nulu pod první prvek v prvním sloupci. Aby se nám to lépe dělalo, prohodíme první řádek s druhým.

$$\sim \left(\begin{array}{rrrrr|r} 2 & -2 & 1 & 0 & 3 & 4 \\ -4 & 4 & -1 & 1 & -7 & -11 \\ 4 & -4 & 5 & 1 & 7 & -3 \\ -6 & 6 & -4 & 1 & -12 & -7 \end{array}\right) \sim$$

Pod dvojkou v prvním sloupci budeme postupně vytvářet nuly. Vezmeme dvojnásobek prvního řádku a přičteme jej ke druhému.

$$\sim \left(\begin{array}{rrrrr|r} 2 & -2 & 1 & 0 & 3 & 4 \\ 0 & 0 & 1 & 1 & -1 & -3 \\ 4 & -4 & 5 & 1 & 7 & -3 \\ -6 & 6 & -4 & 1 & -12 & -7 \end{array}\right) \sim$$

Zatím nemáme v prvním sloupci pod dvojkou všude nuly. Budeme si stále „pomáhat“ násobky prvního řádku, který opíšeme. Minus dvojnásobek prvního řádku přičteme ke třetímu a trojnásobek prvního řádku přičteme ke čtvrtému.

$$\sim \left(\begin{array}{rrrrr|r} 2 & -2 & 1 & 0 & 3 & 4 \\ 0 & 0 & 1 & 1 & -1 & -3 \\ 0 & 0 & 3 & 1 & 1 & -11 \\ 0 & 0 & -1 & 1 & -3 & 5 \end{array}\right) \sim$$

Nyní bychom měli vytvářet nuly ve druhém sloupci. To se v tomto případě stalo (výjimečně) samo, takže se zaměříme na třetí sloupec. Tam pod první jedničkou v druhém řádku vytvoříme nuly takto: minus trojnásobek druhého řádku přičteme ke třetímu a dále druhý řádek přičteme ke čtvrtému. První a druhý řádek opisujeme.

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

Znovu se přesuneme na další sloupec (tentokrát čtvrtý) a vytvoříme nulu pod minus dvojkou ze třetího řádku. K tomu stačí sečíst třetí řádek se čtvrtým a výsledek napsat na místo čtvrtého řádku.

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

Třetí řádek ještě (spíše pro parádu) vynásobíme číslem $-1/2$. Čtvrtý řádek nemusíme psát, protože tento řádek odpovídá rovnici $0x_1 + 0x_2 + 0x_3 + 0x_4 + 0x_5 = 0$, která je zřejmě splněna pro libovolná x_1, x_2, x_3, x_4, x_5.

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

Dostáváme tzv. *schodovitou* matici, která má ve svém „dolním levém koutě“ nuly. Přesněji: každý další řádek má zleva aspoň o jednu nulu více než předešlý. To je cílem tzv. *přímého chodu* Gaussovy eliminační metody, který jsme právě ukončili.

Naši matici koeficientů původní soustavy jsme převedli pomocí Gaussovy eliminační metody na matici odpovídající nové soustavě, která má stejnou množinu řešení, jako původní. Stačí se proto dále zabývat touto novou soustavou. Pro názornost si ji zde zapíšeme

$$\begin{aligned} 2x_1 - 2x_2 + x_3 + 3x_5 &= 4 \\ x_3 + x_4 - x_5 &= -3 \\ x_4 - 2x_5 &= 1 \end{aligned}$$

Každá rovnice umožní spočítat hodnotu jedné neznámé, pokud jsou dány hodnoty ostatních. Máme tři rovnice o pěti neznámých, umíme tedy spočítat jen tři neznámé. Pomocí poslední rovnice budeme počítat například x_4, pomocí předposlední rovnice budeme počítat x_3 a z první rovnice spočítáme například x_1. Ostatní neznámé nejsou těmito rovnicemi určeny a mohou nabývat libovolných hodnot. To dáme najevo například takto: $x_5 = u$, $x_2 = v$, $u \in \mathbf{R}$, $v \in \mathbf{R}$. Nyní budeme počítat hodnoty ostatních neznámých dosazovací metodou, postupujeme od poslední rovnice k první:

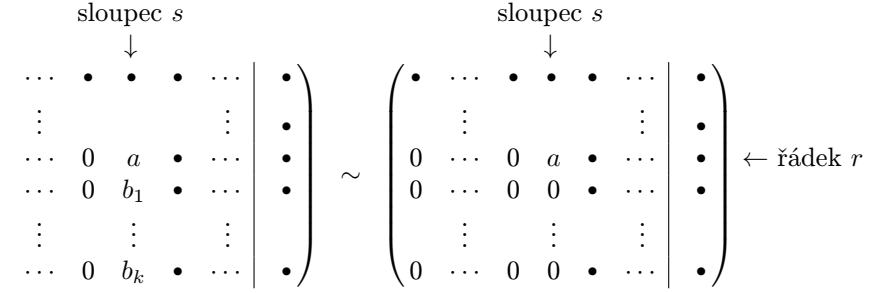
$$\begin{aligned}
&&&& x_5 &= u \\
&&&& x_2 &= v \\
x_4 - 2u &= 1 &\Rightarrow\quad & x_4 &= 1 + 2u \\
x_3 + (1 + 2u) - u &= -3 &\Rightarrow\quad & x_3 &= -4 - u \\
2x_1 - 2v + (-4 - u) + 3u &= 4 &\Rightarrow\quad & x_1 &= 4 - u + v
\end{aligned}$$

Řešení jsme zapsali pomocí dvou parametrů u, v, které mohou nabývat libovolných hodnot. Všimneme si, že počet parametrů, kterými popíšeme řešení libovolné soustavy lineárních rovnic je roven počtu neznámých mínus počet nenulových rovnic, které získáme po přímém chodu Gaussovy eliminační metody. V našem případě: počet parametrů $= 5 - 3$. Zadaná soustava má sice čtyři rovnice, ale po eliminaci se nám soustava redukovala na pouhé tři nenulové rovnice.

Pokud bychom se rozhodli například z první rovnice počítat x_2, pak by neznámá x_1 mohla nabývat libovolných hodnot a výsledek by byl formálně zapsán poněkud jinak: $x_1 = w$,

$x_2 = -8 + 2u + 2w$, $x_3 = -4 - u$, $x_4 = 1 + 2u$, $x_5 = u$, $u \in \mathbf{R}$, $w \in \mathbf{R}$. Vidíme tedy, že neexistuje jednoznačný zápis výsledku. Oba zápisy popisují stejnou množinu řešení, každý trochu jiným způsobem.

Nyní se pustíme do výkladu Gaussovy eliminační metody pro obecnou soustavu lineárních rovnic. Nejprve vysvětlíme proceduru, kterou budeme v této metodě s prvky matice mnohokrát opakovat. Tato procedura vytvoří nuly v s-tém sloupci pod nenulovým prvkem matice v r-tém řádku. Názorně:



Tečkami jsou v tomto obrázku vyznačeny prvky matice, jejichž hodnoty nás momentálně nezajímají. Prvek a musí být nenulový. Procedura „vytvoření nul pod prvkem a“ se provede takto:

K1. Řádky 1 až r opíšeme beze změny.

K2. K řádku $r+1$ přičítáme $(-b_1/a)$ násobek řádku r, k řádku $r+2$ přičítáme $(-b_2/a)$ násobek řádku r, atd., až konečně k řádku poslednímu přičítáme $(-b_k/a)$ násobek řádku r.

Tímto úkonem se neporuší nulové prvky ve sloupcích vlevo od sloupce s a vzniknou nové nuly pod prvkem a ve sloupci s.

Nyní popíšeme přímý chod Gaussovy eliminační metody, který převede libovolnou matici na schodovitou matici, která má „v levém dolním rohu“ nuly. Matice bude mít v každém řádku zleva aspoň o jednu nulu více v souvislé řadě nul, než v předchozím řádku. V algoritmu se pracuje s proměnnou r označující aktuální řádek a s proměnnou s, která znamená sloupec, ve kterém v daném okamžiku vytváříme nuly. Pokud se v algoritmu zvětšuje r, a přitom r již označuje poslední řádek matice, ukončíme činnost. Pokud by se mělo zvětšit s, a přitom s už označuje poslední sloupec matice, ukončíme činnost. V těchto případech je už matice převedena do požadovaného tvaru.

G1. Nastavíme $r = 1$, $s = 1$.

G2. Nechť a je prvek matice z s-tého sloupce a r-tého řádku. Pokud je $a = 0$ a všechny prvky pod prvkem a v s-tém sloupci jsou také nulové, zvětšíme s o jedničku a opakujeme krok G2.

G3. Je-li $a = 0$, a přitom existuje nenulový prvek pod prvkem a v s-tém sloupci na řádku r_1, prohodíme řádek r s řádkem r_1. Od této chvíle je v nové matici prvek na r-tém řádku a s-tém sloupci nenulový.

G4. Vytvoříme nuly pod nenulovým prvkem a z r-tého řádku a s-tého sloupce způsobem, popsaným v krocích K1 a K2.
G5. Existují-li v matici řádky celé nulové, z matice je odstraníme.
G6. Zvětšíme r o jedničku a s o jedničku a celou činnost opakujeme od kroku G2 znova.

Při eliminační metodě jsme převedli matici koeficientů soustavy na jinou matici odpovídající jiné soustavě, ale se stejnou množinou řešení, protože při úpravách jsme použili jen tyto elementární kroky:

(1) Prohození řádků matice.
(2) Pronásobení řádku nenulovou konstantou.
(3) Přičtení násobku řádku k jinému.
(4) Odstranění nulového řádku.

Již dříve jsme vysvětlili, že tím dostáváme modifikovanou matici odpovídající nové soustavě se stejnou množinou řešení. Stačí se tedy zaměřit na tuto novou soustavu. Nejprve rozhodneme, zda soustava má vůbec nějaké řešení. Pokud je poslední řádek ve tvaru:

$$(0 \quad 0 \quad \cdots \quad 0 \mid c), \quad c \neq 0$$

soustava nemá řešení. Tento řádek totiž odpovídá rovnici

$$0x_1 + 0x_2 + \cdots + 0x_n = c, \quad c \neq 0,$$

kterou nelze splnit pro žádná $x_1, x_2, \ldots, x_n$.

Pokud poslední řádek obsahuje nenulový prvek mezi koeficienty soustavy (vlevo od svislé čáry), soustava má řešení. V takovém případě můžeme říci, kolik těch řešení bude: pokud má soustava (po úpravě eliminační metodou) stejný počet rovnic, jako neznámých, má jediné řešení. Je-li počet rovnic menší, než počet neznámých, je řešení nekonečně mnoho.

Počet rovnic po eliminaci nemůže nikdy přesáhnout počet neznámých, vyloučíme-li případ řádku $(0 \ \cdots \ 0 \mid c)$, $c \neq 0$. Rozmyslete si, proč. Zadaná soustava může mít podstatně více rovnic než neznámých, ale po eliminaci se v takovém případě zákonitě počet rovnic zmenší.

Má-li soustava řešení, pak pro každou rovnici rozhodneme, kterou neznámou budeme použitím této rovnice počítat (v dané rovnici musí být tato neznámá násobena nenulovým koeficientem). V každé rovnici je nejprve zleva skupina nulových koeficientů a pak existuje nějaký první nenulový koeficient. Doporučujeme počítat tu neznámou, která je násobena tímto prvním nenulovým koeficientem. Neznámé, které nebudeme počítat pomocí žádné rovnice, mohou nabývat libovolných hodnot. Takové neznámé dále považujeme za parametry. Pro počet parametrů tedy platí:

$$\text{počet parametrů} = \text{počet neznámých celkem} - \text{počet rovnic po eliminaci}$$

Spočítáme nejprve neznámou z poslední rovnice a výsledek dosadíme do ostatních rovnic. Pak spočítáme další neznámou z předposlední rovnice atd. až se dostaneme k první rovnici. Tím máme vyjádřena všechna řešení dané soustavy lineárních rovnic.

Příklad. Gaussovou eliminační metodou budeme řešit následující soustavu čtyř rovnic o čtyřech neznámých $\alpha, \beta, \gamma, \delta$.

$$\begin{aligned} \alpha + 2\beta + 3\gamma + \delta &= 1 \\ 2\alpha + 4\beta + 7\gamma + 7\delta &= 4 \\ \alpha + 2\gamma &= -2 \\ 3\alpha + 7\beta + 10\gamma + 6\delta &= 7 \end{aligned}$$

Zapíšeme koeficienty soustavy a hodnoty pravých stran do matice a začneme tuto matici eliminovat způsobem popsaným výše.

$$\left(\begin{array}{cccc|c} 1 & 2 & 3 & 1 & 1 \\ 2 & 4 & 7 & 7 & 4 \\ 1 & 0 & 2 & 0 & -2 \\ 3 & 7 & 10 & 6 & 7 \end{array}\right) \overset{(1)}{\sim} \left(\begin{array}{cccc|c} 1 & 2 & 3 & 1 & 1 \\ 0 & 0 & 1 & 5 & 2 \\ 0 & -2 & -1 & -1 & -3 \\ 0 & 1 & 1 & 3 & 4 \end{array}\right) \overset{(2)}{\sim} \left(\begin{array}{cccc|c} 1 & 2 & 3 & 1 & 1 \\ 0 & 1 & 1 & 3 & 4 \\ 0 & -2 & -1 & -1 & -3 \\ 0 & 0 & 1 & 5 & 2 \end{array}\right) \overset{(3)}{\sim}$$

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

V úpravě (1) jsme vytvořili nuly pod jedničkou z prvního sloupce a prvního řádku. V úpravě (2) jsme přehodili druhý řádek se čtvrtým v souladu s krokem G3 našeho algoritmu (na

druhém řádku a druhém sloupci totiž byl nulový prvek). V úpravě (3) jsme vytvořili nuly pod jedničkou z druhého řádku v druhém sloupci. V poslední úpravě (4) jsme vytvořili nulu pod jedničkou v třetím sloupci z třetího řádku. Tím máme matici v požadovaném tvaru. Pohledem na poslední řádek okamžitě vidíme, že soustava nemá řešení.

1. Lineární prostor

1.1. Poznámka. *O formě definice-věta-důkaz.* V tomto textu narazíte na tři základní „slohové útvary“: definice, věta a důkaz. Vesměs každé solidní matematické sdělení používá tyto pojmy. Přitom je možné, že s takto systematickým použitím pojmů definice, věta, důkaz se setkáváte poprvé. Proto si tyto pojmy vysvětlíme.

Definice vysvětluje (definuje) nový pojem, který bude dále v teorii používán. Definice se opírá o pojmy, které byly definovány v předchozích definicích. V přísně exaktních teoriích bychom museli na začátku vyjmenovat pojmy, které nedefinujeme, ale budeme s nimi pracovat, protože jinak bychom nebyli schopni zapsat první definici. V tomto textu nebudeme takto přísně exaktní a budeme se opírat o mateřský jazyk a o pojmy známé ze střední školy (předpokládáme, že jsou známé pojmy množina, reálné číslo apod.). Nově definovaný pojem bude v definici vyznačen kurzívou.

Věta je tvrzení, které nám sděluje nějakou vlastnost týkající se definovaných pojmů. Dosti často se věta dá formálně rozčlenit na předpoklady a vlastní tvrzení. Předpoklady bývají uvozeny slovy „nechť“, „budiž“, „jestliže“, „předpokládejme“ atd. Vlastní tvrzení obvykle začíná slovem „pak“ nebo „potom“. Věta se musí dokázat. Proto se hned za větu připojuje další slohový útvar: důkaz. Po dokázání věty se v následujícím textu dá věta *použít*. To bývá obvykle provedeno tak, že se ověří v daném kontextu platnost předpokladů věty a na základě toho se prohlásí, že platí vlastní tvrzení věty.

Důkaz je obhajoba platnosti věty. Při této obhajobě můžeme použít předchozí definice (zaměníme použitý pojem ve větě skupinou pojmů, kterými je pojem definován) a dále můžeme použít dříve dokázané věty (ověříme předpoklady dříve dokázané věty a použijeme pak její vlastní tvrzení). Dále se v důkazech používá logických obratů, které byste měli znát ze střední školy (například výrok „není pravda, že existuje prvek, pro který platí tvrzení A“ lze přeformulovat na totožný výrok: „pro všechny prvky neplatí tvrzení A“).

V exaktních teoriích se ke skupině nedefinovaných pojmů na začátku teorie připojuje i několik tvrzení, která nelze prostředky teorie dokázat, ale pro důkazy dalších vět je nutné jejich platnost předpokládat. Takovým tvrzením se říká axiomy. V našem textu nebudeme teorii stavět jen na axiomech, ale někdy použijeme spíše intuitivní přístup. Není nutné být za každou cenu přísně exaktní.

Pro matematické sdělení nových poznatků je obvykle členění textu na definice, věty a důkazy dostačující. V této učebnici si navíc budeme ilustrovat novou problematiku na *příkladech* a občas prohodíme nějakou *poznámku*. Dokladem toho je i tato poznámka ??.

1.2. Poznámka. V následující definici lineárního prostoru ?? se pracuje s množinami blíže nespecifikovaných objektů. Jediné, co s těmi objekty umíme dělat, je vzájemně objekty sčítat a násobit objekt reálným číslem. Přitom tyto operace (sčítání a násobení reálným číslem) je potřeba pro konkrétní množiny objektů definovat. Pro každou množinu objektů mohou tyto operace vypadat jinak. Skutečnost, že není řečeno, jak objekty a operace s nimi konkrétně

vypadají, může být pro některé čtenáře poněkud frustrující. Proto před definicí uvedeme příklady množin objektů, které lze sčítat a násobit konstantou.

1.3. Příklad. Nechť $\mathbf{R}^2$ je množina všech uspořádaných dvojic reálných čísel. Uspořádanou dvojici zapisujeme ve tvaru (a, b). Vyznačujeme ji tedy kulatou závorkou a její složky a, b píšeme odděleny čárkou. Takže $\mathbf{R}^2 = \{(a, b);\, a \in \mathbf{R}, b \in \mathbf{R}\}$. Symbol $\mathbf{R}$ značí reálná čísla a zápisem $\{X;$ vlastnost $X\}$ značíme množinu objektů X, které mají specifikovanou vlastnost. Definujme sčítání dvou uspořádaných dvojic:

$$(a, b) \oplus (c, d) \stackrel{\text{df}}{=} (a + c, b + d) \tag{1.1}$$

a násobení uspořádané dvojice reálným číslem $\alpha \in \mathbf{R}$:

$$\alpha \odot (a, b) \stackrel{\text{df}}{=} (\alpha\, a, \alpha\, b). \tag{1.2}$$

Všimneme si, že jsme definovali operaci $\oplus$ sčítání objektů tak, že výsledek sčítání je zase uspořádaná dvojice. Stejně součin $\odot$ reálného čísla s uspořádanou dvojicí je zase uspořádaná dvojice, tedy prvek množiny $\mathbf{R}^2$. Naše sčítání je tedy operace, do které vstupují dva prvky množiny $\mathbf{R}^2$ a vystupuje z ní prvek množiny $\mathbf{R}^2$. Naše násobení je operace, do které vstupuje reálné číslo a prvek z $\mathbf{R}^2$ a vystupuje z ní prvek z $\mathbf{R}^2$. Tuto skutečnost zapíšeme pomocí kartézského součinu množin:

$$\oplus : \mathbf{R}^2 \times \mathbf{R}^2 \to \mathbf{R}^2, \qquad \odot : \mathbf{R} \times \mathbf{R}^2 \to \mathbf{R}^2. \tag{1.3}$$

Všimneme si dále, že jsme definovali nové operace $\oplus$ a $\odot$ prostřednictvím operací sčítání a násobení reálných čísel, tj. prostřednicvím operací, jejichž vlastnosti jsou známy ze střední školy. Příkladem takové vlastnosti je komutativní zákon (pro reálná čísla x a y platí: $x+y = y+x$). Naše nově definovaná operace $\oplus$ má také tuto vlastnost:

$$(a,b) \oplus (c,d) = (c,d) \oplus (a,b),$$

protože podle definice je $(a,b)\oplus(c,d) = (a+c, b+d)$ a $(c,d)\oplus(a,b) = (c+a, d+b)$, ovšem dvě uspořádané dvojice se rovnají, pokud se rovnají odpovídající složky. V tomto případě první složka první dvojice $a+b$ se rovná první složce druhé dvojice $b+a$, neboť pro sčítání reálných čísel platí komutativní zákon. Podobně ověříme i druhou složku.

Uvědomíme si, že není vůbec automaticky zaručeno, že nově definované operace musejí tyto zákony splňovat. Pokud bychom například definovali jiné sčítání dvou uspořádaných dvojic předpisem:

$$(a,b) \mathbin{\underline{\oplus}} (c,d) \stackrel{\text{df}}{=} (2a+d, b+c), \tag{1.4}$$

pak se dá snadno ukázat, že pro $\underline{\oplus}$ není splněn komutativní zákon (ověřte si sami).

1.4. Příklad. Označme P množinu všech reálných polynomů, tedy funkcí $p\colon \mathbf{R} \to \mathbf{R}$, které pro $x \in \mathbf{R}$ mají hodnotu danou vzorcem:

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad (a_n, a_{n-1}, \ldots, a_1, a_0 \text{ jsou nějaká reálná čísla}). \tag{1.5}$$

Na této množině polynomů definujeme sčítání $\oplus\colon P \times P \to P$ a násobení $\odot\colon \mathbf{R} \times P \to P$ takto: pro každé $p \in P$, $q \in P$, $\alpha \in \mathbf{R}$ je

$$(p \oplus q)(x) \stackrel{\text{df}}{=} p(x) + q(x) \qquad \forall x \in \mathbf{R},$$
$$(\alpha \odot p)(x) \stackrel{\text{df}}{=} \alpha\, p(x) \qquad \forall x \in \mathbf{R}.$$

Řečeno pečlivěji: v definici jsme zavedli novou funkci $p \oplus q\colon \mathbf{R} \to \mathbf{R}$ tak, že jsme řekli, jakou bude tato funkce mít hodnotu v každém bodě x jejího definičního oboru. Tuto hodnotu podle definice počítáme jako součet hodnoty funkce p a hodnoty funkce q v bodě x. Tyto hodnoty jsou reálná čísla, takže sčítání funkcí (nové sčítání nových objektů) vlastně definujeme pomocí sčítání reálných čísel (sčítání, které známe ze střední školy). Podobně definujeme násobek funkce reálným číslem.

Dá se ověřit, že pro $p \in P$, $q \in P$, $\alpha \in \mathbf{R}$ je $p \oplus q$ zase polynom a $\alpha \odot p$ je také polynom. Rovněž se dá ověřit, že pro operaci $\oplus$ platí komutativní zákon.

1.5. Poznámka. V předchozích dvou příkladech jsme definovali na množině nějakých objektů sčítání a násobení reálným číslem. Pro větší přehlednost jsme nově definované operace zapisovali do kroužku, abychom je odlišili od operací sčítání a násobení reálných čísel. To ale není potřeba. Stačí používat tytéž znaky, protože podle typu objektů, které do operace vstupují, okamžitě poznáme, jakou operaci máme použít (zda nově definovanou nebo známou operaci

na reálných číslech). Takové automatické přizpůsobení operace podle typu operandů znají programátoři objektově orientovaných jazyků. Tam se tomu říká „přetěžování operátorů“.

Definici sčítání uspořádaných dvojic tedy stačí zapsat takto: Pro všechna $(a,b) \in \mathbf{R}^2, (c,d) \in \mathbf{R}^2$ je $(a,b)+(c,d) \stackrel{\text{df}}{=} (a+c, b+d)$. Přitom poznáme, že první znak „+“ v uvedeném vzorci označuje sčítání uspořádaných dvojic a ostatní dva znaky „+“ znamenají sčítání reálných čísel.

V dalším textu budeme skoro vždy používat znaky „+“ a „$\cdot$“ i pro nově definované operace, protože podle typu operandů nemůže dojít k nedorozumění. Také znak násobení „$\cdot$“ budeme někdy vynechávat, jako jsme zvyklí jej vynechávat při zápisu násobení reálných čísel.

1.6. Definice.* *Lineárním prostorem* nazýváme každou neprázdnou množinu L, na které je definováno sčítání $+ \colon L \times L \to L$ a násobení reálným číslem $\cdot \colon \mathbf{R} \times L \to L$ a tyto operace

splňují pro každé $\boldsymbol{x} \in L, \boldsymbol{y} \in L, \boldsymbol{z} \in L, \alpha \in \mathbf{R}, \beta \in \mathbf{R}$ vlastnosti:

(1)	$\boldsymbol{x} + \boldsymbol{y} = \boldsymbol{y} + \boldsymbol{x}$	(komutativní zákon sčítání),
(2)	$(\boldsymbol{x} + \boldsymbol{y}) + \boldsymbol{z} = \boldsymbol{x} + (\boldsymbol{y} + \boldsymbol{z})$	(asociativní zákon sčítání),
(3)	$\alpha \cdot (\beta \cdot \boldsymbol{x}) = (\alpha\beta) \cdot \boldsymbol{x}$	(asociativní zákon násobení),
(4)	$\alpha \cdot (\boldsymbol{x} + \boldsymbol{y}) = \alpha \cdot \boldsymbol{x} + \alpha \cdot \boldsymbol{y}$	(distributivní zákon pro sčítání prvk
(5)	$(\alpha + \beta) \cdot \boldsymbol{x} = \alpha \cdot \boldsymbol{x} + \beta \cdot \boldsymbol{x}$	(distributivní zákon pro sčítání čísel
(6)	$1 \cdot \boldsymbol{x} = \boldsymbol{x}$	(vlastnost reálného čísla 1),
(7)	existuje $\boldsymbol{o} \in L$, že pro každé $\boldsymbol{x} \in L$ je $0 \cdot \boldsymbol{x} = \boldsymbol{o}$	(existence nulového prvku).

Prvky lineárního prostoru nazýváme *vektory*. Reálnému číslu v kontextu násobení $\cdot : \mathbf{R} \times L \to L$ říkáme *skalár*. Prvku $\boldsymbol{o} \in L$ z vlastnosti (7) říkáme *nulový prvek* nebo *nulový vektor*.

1.7. Věta. Pro nulový prvek $\boldsymbol{o}$ lineárního prostoru L platí vlastnosti:

(1) $\boldsymbol{x} + \boldsymbol{o} = \boldsymbol{x} \qquad \forall\, \boldsymbol{x} \in L,$

(2) $\alpha \cdot \boldsymbol{o} = \boldsymbol{o} \qquad \forall\, \alpha \in \mathbf{R},$

(3) Nechť $\boldsymbol{x} \in L$. Je-li $\alpha \cdot \boldsymbol{x} = \boldsymbol{o}$ a $\alpha \neq 0$, pak $\boldsymbol{x} = \boldsymbol{o}$.

Důkaz. Použijeme vlastnosti z definice ??. Pro přehlednost píšeme nad rovnítka číslo použité vlastnosti.

(1) $\boldsymbol{x} + \boldsymbol{o} \overset{(7)}{=} \boldsymbol{x} + 0 \cdot \boldsymbol{x} \overset{(6)}{=} 1 \cdot \boldsymbol{x} + 0 \cdot \boldsymbol{x} \overset{(5)}{=} (1+0) \cdot \boldsymbol{x} = 1 \cdot \boldsymbol{x} \overset{(6)}{=} \boldsymbol{x}.$

(2) $\alpha \cdot \boldsymbol{o} \overset{(7)}{=} \alpha \cdot (0 \cdot \boldsymbol{x}) \overset{(3)}{=} (\alpha \cdot 0) \cdot \boldsymbol{x} = 0 \cdot \boldsymbol{x} \overset{(7)}{=} \boldsymbol{o}.$

(3) $\boldsymbol{x} \overset{(6)}{=} 1 \cdot \boldsymbol{x} = \left(\frac{1}{\alpha}\,\alpha\right) \cdot \boldsymbol{x} \overset{(3)}{=} \frac{1}{\alpha} \cdot (\alpha \cdot \boldsymbol{x}) \overset{\text{(z předpokladu)}}{=} \frac{1}{\alpha} \cdot \boldsymbol{o} \overset{\text{(vlastnost (2) věty ??)}}{=} \boldsymbol{o}.$

1.8. Poznámka. Ve vlastnostech (1) až (7) v definici ?? se pracuje se znaky „+“ a „·“ v souladu s poznámkou ?? ve dvojím významu. Buď to jsou operace s prvky množiny L nebo operace s reálnými čísly. Například ve vlastnosti (5) je první symbol „+“ použit ve významu sčítání na množině reálných čísel, zatímco druhý symbol „+“ je použit ve významu sčítání na množině L. Jako cvičení zkuste o každé použité operaci ve vzorcích (1) až (7) rozhodnout, jakého je druhu.

1.9. Poznámka. Protože lineární prostor obsahuje vektory, v literatuře se často setkáváme s pojmem *vektorový prostor*, který je použit v naprosto stejném smyslu, jako zde používáme pojem *lineární prostor*. Je třeba si uvědomit, že *vektory* v tomto pojetí nejsou jen „šipky“, ale jakékoli matematické objekty, které umíme mezi sebou sčítat a násobit skalárem tak, že tyto operace splňují *axiomy linearity* (1) až (7) z definice ??. Následující příklady ukazují, že lze v matematice najít skutečně rozličné případy lineárních (vektorových) prostorů.

1.10. Příklad. Ukážeme, že množina $\mathbf{R}^2$ z příkladu ?? se sčítáním a násobením skalárem podle definic (1.1) a (1.2) tvoří lineární prostor. Místo znaků „$\oplus$“ a „$\odot$“ budeme nadále používat znaky„$+$“ a „$\cdot$“.

Nejprve je třeba zjistit, zda operace „$+$“ a „$\cdot$“ jsou skutečně definovány způsobem, jak požaduje definice ??, tj. zda platí $+ \colon \mathbf{R}^2 \times \mathbf{R}^2 \to \mathbf{R}^2$ a $\cdot \colon \mathbf{R} \times \mathbf{R}^2 \to \mathbf{R}^2$. To jsme ale už ověřili dříve, viz (1.3).

Dále zjistíme platnost vlastností (1) až (7) z definice ??. Vlastnost (1) jsme podrobně ověřovali v příkladu ??. Pokračujeme tedy vlastností (2). Pro každé $a, b, c, d, e, f \in \mathbf{R}$ platí:

$$\begin{aligned}\big((a,b)+(c,d)\big)+(e,f) &= (a+c,b+d)+(e,f) = \big((a+c)+e,(b+d)+f\big) = \\ &= \big(a+(c+e),b+(d+f)\big) = (a,b)+(c+e,d+f) = (a,b)+\big((c,d)+\end{aligned}$$

Při úpravách jsme nejprve dvakrát použili definici (1.1), pak jsme v jednotlivých složkách využili toho, že pro sčítání reálných čísel platí asociativní zákon a konečně jsme zase dvakrát

použili definici (1.1). Nyní dokážeme další vlastnosti. Pro každé $a, b, c, d, \alpha, \beta \in \mathbf{R}$ platí:

(3) $\alpha \cdot \big(\beta \cdot (a,b)\big) = \alpha \cdot \big(\beta\, a, \beta\, b\big) = \big(\alpha\,(\beta\, a), \alpha\,(\beta\, b)\big) = \big((\alpha\,\beta)\, a, (\alpha\,\beta)\, b\big) = (\alpha\,\beta)\,(a,b),$

(4) $\alpha \cdot \big((a,b) + (c,d)\big) = \alpha \cdot (a+c, b+d) = \big(\alpha\,(a+c), \alpha\,(b+d)\big) = (\alpha\, a + \alpha\, c, \alpha\, b + \alpha\, d) =$
$= (\alpha\, a, \alpha\, b) + (\alpha\, c, \alpha\, d) = \alpha\,(a,b) + \alpha\,(c,d),$

(5) $(\alpha+\beta) \cdot (a,b) = \big((\alpha+\beta)\, a, (\alpha+\beta)\, b\big) = (\alpha\, a + \beta\, a, \alpha\, b + \beta\, b) = (\alpha\, a, \alpha\, b) + (\beta\, a, \beta\, b) =$
$= \alpha\,(a,b) + \beta\,(a,b),$

(6) $1 \cdot (a,b) = (1\, a, 1\, b) = (a,b),$

(7) dvojice $(0,0)$ splňuje: $(0,0) = 0 \cdot (a,b)$, protože $0 \cdot (a,b) = (0\, a, 0\, b) = (0,0)$.

Použili jsme nejprve definice (1.1) a (1.2), pak jsme využili vlastnosti reálných čísel v jednotlivých složkách dvojice. Nakonec jsme znovu použili definice (1.1) a (1.2).

Vidíme, že nulovým vektorem lineárního prostoru $\mathbf{R}^2$ je dvojice $(0,0)$. Podle konvence ze závěru definice ?? jsme oprávněni uspořádaným dvojicím se sčítáním a násobením podle definic (1.1) a (1.2) říkat vektory.

1.11. Příklad. Množina $\mathbf{R}^2$ se sčítáním $\underline{\oplus}$ podle definice (1.4) a násobením $\odot$ podle (1.2) netvoří lineární prostor. Není totiž splněna například vlastnost (1) z definice ??.

1.12. Příklad.* Znakem $\mathbf{R}^n$ označíme množinu všech uspořádaných n-tic reálných čísel, (n je nějaké přirozené číslo, $n \geq 1$). Jinými slovy:

$$\mathbf{R}^n = \{(a_1, a_2, \ldots, a_n);\, a_1 \in \mathbf{R},\, a_2 \in \mathbf{R}, \ldots,\, a_n \in \mathbf{R}\}.$$

Definujme $+\colon \mathbf{R}^n \times \mathbf{R}^n \to \mathbf{R}^n$, $\cdot\colon \mathbf{R} \times \mathbf{R}^n \to \mathbf{R}^n$ takto: pro každé $(a_1, \ldots, a_n) \in \mathbf{R}^n$, $(b_1, \ldots, b_n) \in \mathbf{R}^n$, $\alpha \in \mathbf{R}$ je

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) \stackrel{\text{df}}{=} (a_1 + b_1, \ldots, a_n + b_n),$$

$$\alpha \cdot (a_1, \ldots, a_n) \stackrel{\text{df}}{=} (\alpha\, a_1, \ldots, \alpha\, a_n).$$

Množina $\mathbf{R}^n$ s takto definovanými operacemi tvoří lineární prostor.

Důkaz bychom provedli analogicky jako v příkladu ??, ale pro úsporu místa to již nebudeme opakovat. Vidíme tedy, že uspořádané n-tice s takto definovaným sčítáním a násobením skalárem můžeme nazývat vektory. Speciálně v případě uspořádaných n-tic mluvíme o *aritmetických vektorech*. Číslo a_i nazýváme *i-tou složkou vektoru* $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$.

1.13. Příklad. Množina $\mathbf{R}$ s obvyklým sčítáním reálných čísel a násobením reálného čísla reálným číslem tvoří lineární prostor. To je zřejmé. Sčítání a násobení reálných čísel totiž splňuje vlastnosti (1) až (7) z definice ??. Tento poznatek si jistě přinášíte ze střední školy. V tomto textu jsme jej už použili, když jsme ověřovali, že $\mathbf{R}^2$ nebo $\mathbf{R}^n$ je lineární prostor.

Nulovým prvkem lineárního prostoru $\mathbf{R}$ je číslo 0. V kontextu sčítání a násobení můžeme tedy říkat reálným číslům vektory, ale obvykle to neděláme.

1.14. Příklad. Zvolme jeden bod v prostoru, který nás obklopuje, a označme jej písmenem O. Uděláme to třeba tak, že nakreslíme na papír křížek a prohlásíme jej za bod O. Uvažujme všechny orientované úsečky, které začínají v bodě O a končí v nějakém jiném bodě v prostoru. Přidejme k tomu „degenerovanou“ úsečku, která začíná i končí v bodě O a označme množinu všech těchto úseček znakem U_O.

Definujme nyní sčítání $+ \colon U_O \times U_O \to U_O$ ryze konstruktivně takto: Úsečky $\boldsymbol{u} \in U_O$, $\boldsymbol{v} \in U_O$ doplníme na rovnoběžník. Úhlopříčku, která začíná v bodě O a končí v protějším bodě rovnoběžníka, prohlásíme za součet úseček $\boldsymbol{u}$ a $\boldsymbol{v}$, tedy $\boldsymbol{u} + \boldsymbol{v}$. Dále definujme násobení skalárem $\cdot \colon \mathbf{R} \times U_O \to U_O$ takto: Úsečkou $\boldsymbol{u}$ proložíme přímku, na kterou nekreslíme číselnou osu s nulou v bodě O a jedničkou v koncovém bodě úsečky $\boldsymbol{u}$. Na ose najdeme bod (číslo) α. Úsečka, která končí v tomto bodě je vektor $\alpha \cdot \boldsymbol{u}$. Je-li $\boldsymbol{u}$ degenerovaná úsečka končící v bodě O, pak $\alpha \cdot \boldsymbol{u}$ definujeme jako stejnou degenerovanou úsečku končící v bodě O.

Množina U_O s takto konstruktivně definovaným sčítáním a násobením reálným číslem tvoří lineární prostor. Je zřejmé, že součet orientovaných úseček je orientovaná úsečka a α násobek orientované úsečky je orientovaná úsečka. Ještě ověříme vlastnosti (1) až (7) z definice ??. (1) $\boldsymbol{u} + \boldsymbol{v} = \boldsymbol{v} + \boldsymbol{u}$, protože v obou případech doplňujeme na stejný rovnoběžník. (2) $(\boldsymbol{u} + \boldsymbol{v}) + \boldsymbol{w} = \boldsymbol{u} + (\boldsymbol{v} + \boldsymbol{w})$, protože postupné doplnění úhlopříčky rovnoběžníku $\boldsymbol{u}, \boldsymbol{v}$ a úsečky $\boldsymbol{w}$ na rovnoběžník vede ke stejnému výsledku, jako když nejprve sestavíme úhlopříčku rovnoběžníku $\boldsymbol{v}, \boldsymbol{w}$ a tu doplníme na rovnoběžník s úsečkou $\boldsymbol{u}$ (udělejte si náčtrek). Výsledný součet je tělesová úhlopříčka rovnoběžnostěnu, který je vymezen úsečkami $\boldsymbol{u}$, $\boldsymbol{v}$ a $\boldsymbol{w}$. (3) $\alpha \cdot (\beta \boldsymbol{u}) = (\alpha\, \beta) \cdot \boldsymbol{u}$, protože na levé straně rovnosti se pracuje s měřítkem, které je βkrát

větší než původní měřítko. Na původním měřítku se hledá bod $\alpha\beta$ a na βkrát větším měřítku se hledá bod α. (4) $\alpha \cdot (\boldsymbol{u} + \boldsymbol{v}) = \alpha \cdot \boldsymbol{u} + \alpha \cdot \boldsymbol{v}$, protože příslušné rovnoběžníky pro sčítání jsou podobné a druhý je α krát větší než první. Proto též jeho úhlopříčka bude α krát větší. (5) $(\alpha + \beta) \cdot \boldsymbol{u} = \alpha \cdot \boldsymbol{u} + \beta \cdot \boldsymbol{u}$, protože sečtení vektorů $\alpha \cdot \boldsymbol{u} + \beta \cdot \boldsymbol{u}$ probíhá v „degenerovaném“ rovnoběžníku, který se celý vejde do přímky. Na ní se sčítají úsečky o velikostech α a β, takže dostáváme na měřítku bod $\alpha + \beta$. (6) $1 \cdot \boldsymbol{u} = \boldsymbol{u}$, protože jednička na měřítku leží v koncovém bodě vektoru $\boldsymbol{u}$. (7) $0 \cdot \boldsymbol{u}$ je vždy úsečka kočící v bodě O, protože tam je nula pomyslného měřítka. Degenerovaná úsečka začínající i končící v bodě O je tedy nulovým prvkem našeho lineárního prostoru.

Vidíme, že orientované úsečky s výše definovaným geometrickým sčítáním a násobením skalárem můžeme v souladu s definicí ?? nazývat vektory. Zatímco v příkladu ?? jsme definovali sčítání vektorů a násobení konstantou numericky (v jednotlivých složkách sčítáme reálná čísla), v případě lineárního prostoru U_O jsou tyto operace definovány zcela jinak: geometricky.

1.15. Příklad. Uvažujme množinu F_D všech reálných funkcí reálné proměnné definovaných na nějaké množině $D \subseteq \mathbf{R}$, tj. $F_D = \{f;\, f : D \to \mathbf{R}\}$. Pro libovolné funkce $f \in F_D$, $g \in F_D$ a pro libovolné reálné číslo α definujme součet $f + g$ a násobek skalárem $\alpha \cdot f$ takto:

$$(f + g)(x) \stackrel{\text{df}}{=} f(x) + g(x) \qquad \forall x \in D \tag{1.6}$$

$$(\alpha \cdot f)(x) \stackrel{\text{df}}{=} \alpha\, f(x) \qquad \forall x \in D \tag{1.7}$$

(srovnejte s definicí $\oplus$ a $\odot$ v příkladu ??). Ukážeme, že množina F_D s takto definovaným sčítáním a násobením skalárem tvoří lineární prostor.

Potřebujeme ověřit, zda součet funkcí z množiny F_D je opět funkce z množiny F_D a skalární násobek je také funkce z F_D. To ale platí, protože sčítáním funkcí ani násobením funkce konstantou podle naší definice se nemění definiční obor a výsledkem operací je znovu reálná funkce reálné proměnné.

Dále potřebujeme ověřit vlastnosti (1) až (7) z definice ??. Pro libovolné $f \in F_D, g \in F_D, h \in$ $\alpha \in \mathbf{R}, \beta \in \mathbf{R}$ a pro všechna $x \in D$ platí:

1) $(f+g)(x) = f(x) + g(x) = g(x) + f(x) = (g+f)(x)$,

2) $\big((f+g)+h\big)(x) = (f+g)(x) + h(x) = \big(f(x)+g(x)\big) + h(x) = f(x) + \big(g(x)+h(x)\big) =$
$= f(x) + (g+h)(x) = \big(f+(g+h)\big)(x)$,

3) $\big(\alpha \cdot (\beta \cdot f)\big)(x) = \alpha\,\big((\beta \cdot f)(x)\big) = \alpha\,\big(\beta\, f(x)\big) = (\alpha\,\beta) f(x) = \big((\alpha\,\beta)\cdot f\big)(x)$,

4) $\big(\alpha \cdot (f+g)\big)(x) = \alpha\,\big((f+g)(x)\big) = \alpha\,(f(x)+g(x)) = \alpha\, f(x) + \alpha\, g(x) =$
$= (\alpha \cdot f)(x) + (\alpha \cdot g)(x) = (\alpha \cdot f + \alpha \cdot g)(x)$,

5) $\big((\alpha+\beta)\cdot f\big)(x) = (\alpha+\beta)\, f(x) = \alpha\, f(x) + \beta\, f(x) = (\alpha \cdot f)(x) + (\beta \cdot f)(x) = (\alpha \cdot f + \beta \cdot f)(x$

6) $(1 \cdot f)(x) = 1 \cdot f(x) = f(x)$,

7) $(0 \cdot f)(x) = 0 \cdot f(x) = o(x)$, kde funkce o má pro všechna $x \in D$ hodnotu 0.

Ačkoli tyto vzorce vypadají na první pohled jen jako „hraní se závorkami“, musíme si uvědomit, že rovnost funkcí zde dokazujeme na základě rovnosti jejich hodnot v každém bodě $x \in D$ a že při důkazu používáme nejprve rozepsání operací podle vzorců (1.6) a (1.7). Tím problém převádíme na sčítání a násobení reálných čísel, kde jsou vlastnosti (1) až (7) zaručeny. Jako cvičení si zkuste přepsat tyto vzorce tak, že odlišíte operace sčítání funkcí a násobení funkce skalárem od běžných operací „$+$“ a „$\cdot$“ pro reálná čísla. Použijte například symbolů $\oplus$ a $\odot$, jako v příkladu ??.

Vidíme, že množina F_D s definicí sčítání a násobení skalárem podle vzorců (1.6) a (1.7) je lineárním prostorem. Funkce z F_D jsme tedy podle definice ?? oprávněni nazývat vektory. Nulovým vektorem je v tomto případě funkce, která má pro všechna $x \in D$ nulovou hodnotu.

1.16. Příklad. Ukážeme, že množina P všech polynomů s definicemi sčítání a násobení skalárem podle příkladu ?? tvoří lineární prostor.

Především součet dvou polynomů je polynom a skalární násobek polynomu je polynom, takže platí, že $+ \colon P \times P \to P$ a $\cdot \colon \mathbf{R} \times P \to P$. To je ale vše, co potřebujeme dokázat. Ověřováním vlastností (1) až (7) se nemusíme zdržovat, protože jsme definice sčítání a násobení polynomů převzali z prostoru funkcí F_D, o němž jsme dokázali v příkladu ??, že se jedná o lineární prostor (volíme $D = \mathbf{R}$). Při ověřování vlastností (1) až (7) bychom dělali vlastně to samé jako v příkladu ??, jen na podmnožině $P \subseteq F_D$.

1.17. Příklad. Nechť $n \in \mathbf{N}$, $n \geq 0$ (symbolem $\mathbf{N}$ značíme množinu přirozených čísel). Množina P_n všech polynomů právě n-tého stupně s definicemi sčítání a násobení skalárem podle příkladu ?? *netvoří* lineární prostor. Připomeneme, že *stupeň polynomu* se definuje jako největší $k \in \mathbf{N}$ takové, že a_k je ve vzorci (1.5) nenulové. Jsou-li všechna a_k nulová, definujeme stupeň takového polynomu jako -1.

Proč není množina P_n lineárním prostorem? Sečteme-li totiž dva polynomy n-tého stupně, například x^n+2 a $-x^n-2$, dostáváme nulový polynom, což je polynom stupně -1. Tento protipříklad ukazuje, že neplatí vlastnost $+ : P_n \times P_n \to P_n$. Dokonce neplatí ani $\cdot : \mathbf{R} \times P_n \to P_n$ (zkuste násobit polynom n-tého stupně nulou).

1.18. Poznámka. Příklady ?? a ?? ukazují, že můžeme vymezit podmnožinu $M \subseteq L$ lineárního prostoru L a převzít pro ni operace sčítání a násobení konstantou z L. Za jistých okolností množina M s převzatými operacemi může být lineárním prostorem, ale nemusí být vždy. Z příkladu ?? navíc vidíme, že stačí ověřit vlastnosti $+ : M \times M \to M$ a $\cdot : \mathbf{R} \times M \to M$, abychom mohli prohlásit, že M je lineární prostor. Vlastnosti (1) až (7) není třeba znovu ověřovat, protože operace neměníme. Podmožinu lineárního prostoru, která je sama lineárním prostorem při použití stejných operací, nazýváme lineárním podprostorem. Přesněji viz následující definici.

1.19. Definice. Nechť L je lineární prostor s operacemi „+“ a „$\cdot$“. Neprázdnou množinu $M \subseteq L$ nazýváme *lineárním podprostorem prostoru L*, pokud pro všechna $\boldsymbol{x} \in M, \boldsymbol{y} \in M$ a

$\alpha \in \mathbf{R}$ platí:

$$(1) \quad \boldsymbol{x} + \boldsymbol{y} \in M,$$
$$(2) \quad \alpha \cdot \boldsymbol{x} \in M.$$

1.20. Příklad. Množina všech polynomů P z příkladu ?? je lineárním podprostorem množiny všech funkcí F_D z příkladu ??, kde volíme $D = \mathbf{R}$. Množina P_n všech polynomů právě n-tého stupně z příkladu ?? není lineárním podprostorem lineárního prostoru F_D ani lineárního prostoru P.

1.21. Příklad. Množina $P_{\leq n}$ všech polynomů nejvýše n-tého stupně je lineárním podprostorem lineárního prostoru všech polynomů P i lineárního prostoru všech reálných funkcí F_D. Je to dáno tím, že (1) součtem polynomů nejvýše n-tého stupně dostáváme polynom nejvýše n-tého stupně a (2) vynásobením polynomu nejvýše n-tého stupně reálným číslem dostaneme zase polynom nejvýše n-tého stupně.

1.22. Příklad. Uvažujme $M \subseteq \mathbf{R}^n$, $M = \{(a, a, \ldots, a);\ a \in \mathbf{R}\}$. Předpokládáme tedy, že množina M obsahuje takové n-tice, ve kterých se všechny složky vzájemně rovnají. Ukážeme, že M je lineární podprostor lineárního prostoru $\mathbf{R}^n$.

Stačí pro množinu M dokázat vlastnosti (1) a (2) z definice ??. Platí (1) součet dvou uspořádaných n-tic, ve kterých se složky rovnají, je uspořádaná n-tice, ve kterých se složky

rovnají. (2) vynásobením uspořádané n-tice, ve které se složky rovnají, reálným číslem, dostáváme zase uspořádanou n-tici, ve které se složky rovnají.

1.23. Příklad. Uvažujme množiny $M \subseteq \mathbf{R}^3$, $N \subseteq \mathbf{R}^3$ a $S \subseteq \mathbf{R}^3$, které jsou definovány takto:

$$M = \{(x, y, z);\ x + 2y = 0,\ z \text{ libovolné}\},$$
$$N = \{(x, y, z);\ 2x + y - z = 0\},$$
$$S = \{(x, y, z);\ 2x + y - z = 3\}.$$

Ukážeme, že M a N jsou lineárními podprostory lineárního prostoru $\mathbf{R}^3$, zatímco S není lineárním podprostorem lineárního prostoru $\mathbf{R}^3$.

Ověříme vlastnost (1) z definice ??: Nechť $(x_1, y_1, z_1) \in M$ a $(x_2, y_2, z_2) \in M$. Pak platí $x_1 + 2y_1 = 0$ a $x_2 + 2y_2 = 0$. Pro součet $(x_1 + x_2, y_1 + y_2, z_1 + z_2)$ platí $x_1 + 2y_1 + x_2 + 2y_2 = 0$ (sečetli jsme předchozí rovnice), tj. $(x_1 + x_2) + 2(y_1 + y_2) = 0$, takže i součet leží v množině M. Nyní vlastnost (2): Jestliže $(x, y, z) \in M$, $\alpha \in \mathbf{R}$, pak platí $x + 2y = 0$. Vynásobením rovnice číslem α dostáváme, že též $\alpha\, x + 2\alpha\, y = 0$, což ale znamená, že i trojice $\alpha \cdot (x, y, z)$ leží v množině M. Ověření, že množina N je lineárním podprostorem, lze provést podobně.

Množina S není lineárním podprostorem, protože například $0 \cdot (x, y, z) = (0, 0, 0)$, což je ale prvek, který neleží v S. Neplatí totiž $2 \cdot 0 + 0 - 0 = 3$.

1.24. Věta.* Nechť $M \subseteq L$ a $N \subseteq L$ jsou lineární podprostory lineárního prostoru L. Pak platí:

(1) $M \cap N$ je lineární podprostor lineárního prostoru L.

(2) $M \cup N$ nemusí být lineární podprostor lineárního prostoru L.

Důkaz. (1) Z předpokladů věty a definice ?? víme, že pro $\boldsymbol{x} \in M$, $\boldsymbol{y} \in M$, $\alpha \in \mathbf{R}$ je $\boldsymbol{x}+\boldsymbol{y} \in M$ a $\alpha \cdot \boldsymbol{x} \in M$. Totéž platí pro množinu N. Pokud nyní $\boldsymbol{x} \in M \cap N$, $\boldsymbol{y} \in M \cap N$, pak $\boldsymbol{x}$ i $\boldsymbol{y}$ leží současně v M i N, takže platí, že $\boldsymbol{x}+\boldsymbol{y} \in M$, $\alpha \cdot \boldsymbol{x} \in M$ a současně $\boldsymbol{x}+\boldsymbol{y} \in N$, $\alpha \cdot \boldsymbol{x} \in N$. Prvky $\boldsymbol{x}+\boldsymbol{y}$ a $\alpha \cdot \boldsymbol{x}$ leží v obou množinách M a N současně a to není jinak možné, než že leží v průniku těchto množin.

(2) Abychom ukázali, že sjednocení $M \cup N$ nemusí být lineárním podprostorem, stačí najít vhodný příklad. Nechť $M = \{(a,0);\, a \in \mathbf{R}\}$, $N = \{(0,b);\, b \in \mathbf{R}\}$. Je zřejmé, že M a N jsou lineárními podprostory lineárního prostoru $\mathbf{R}^2$. Sjednocením těchto množin je množina uspořádaných dvojic, pro které je první nebo druhá složka nulová. Vezmeme nyní $(1,0) \in M \cup N$ a $(0,1) \in M \cup N$. Součet $(1,0)+(0,1) = (1,1)$ je uspořádaná dvojice, která neleží ve sjednocení $M \cup N$.

1.25. Příklad. Uvažujme podprostory M a N z příkladu ??. Podle věty ?? je také $M \cap N$ lineárním podprostorem lineárního prostoru $\mathbf{R}^3$.

1.26. Příklad. Nechť U_O je lineární prostor orientovaných úseček zavedený v příkladu ?? a dále nechť $M \subset U_O$ jsou jen takové úsečky, které leží ve stejné rovině, jako leží náš papír, na který jsme v příkladu ?? nakreslili křížek. Vidíme, že $M \neq U_O$, protože například úsečka nenulové velikosti kolmá na náš papír neleží v M. Ukážeme, že množina M je lineární podprostor lineárního prostoru U_O. Skutečně, součet libovolných dvou úseček leží ve stejné rovině (protože tam leží celý rovnoběžník) a násobek úsečky leží dokonce na stejné přímce, jako původní úsečka, takže nutně zůstává ve stejné rovině.

Každá rovina, která prochází bodem O, obsahuje podmnožinu úseček z U_O, které tvoří lineární podprostor lineárního prostoru U_O.

Uvažujme nyní dvě roviny, které mají společný bod O, ale nejsou totožné. Jejich průnik je nějaká přímka, procházející bodem O. Všechny orientované úsečky z U_O, které leží v této přímce, tvoří podle věty ?? rovněž lineární podprostor lineárního prostoru U_O.

1.27. Příklad. Nekonečné posloupnosti reálných čísel lze sčítat tak, že sčítáme odpovídající prvky jednotlivých posloupností. A můžeme je násobit konstantou tak, že všechny prvky posloupnosti jsou vynásobeny touto konstantou. Tedy:

$$(a_1, a_2, a_3, a_4, \ldots) + (b_1, b_2, b_3, b_4, \ldots) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, a_4 + b_4, \ldots),$$
$$\alpha \cdot (a_1, a_2, a_3, a_4, \ldots) = (\alpha a_1, \alpha a_2, \alpha a_3, \alpha a_4, \ldots).$$

Množina nekonečných posloupností S s takto zavedenými operacemi sčítání a násobení konstantou tvoří lineární prostor. Argumentuje se stejně, jako v příkladu ??.

Podmnožina $C \subseteq S$ nekonečných posloupností, které jsou konvergentní, tvoří lineární podprostor lineárního prostoru S, neboť součet konvergentních posloupností je konvergentní posloupnost a násobek konvergentní posloupnosti je konvergentní posloupnost.

Podmnožina $N \subseteq S$ nekonečných posloupností, které mají limitu nula, tvoří lineární podprostor lienárního prostoru S, neboť součet posloupností majících limitu nula je posloupnost mající limitu nula a násobek posloupnosti s limitou nula je posloupnost s limitou nula. Dokonce N je lineárním podprostorem lineárního prostoru C.

Nekonečné posloupnosti, které mají jen konečně mnoho nenulových prvků, se nazývají *posloupnosti s konečným nosičem*. Podmnožina $K \subseteq S$ posloupností s konečným nosičem tvoří lineární podprostor, neboť součet posloupností s konečným nosičem je posloupnost s konečným nosičem a násobek posloupnosti s konečným nosičem je posloupnost s konečným nosičem. Dokonce K je lineárním podprostorem lineárního prostoru N.

Stručně: K je podprostorem N je podprostorem C je podprostorem S.

1.28. Poznámka. Zamysleme se, jak může vypadat lineární prostor s nejmenším počtem prvků. Podle definice ?? je lineární prostor vždy neprázdná množina, takže musí obsahovat aspoň jeden prvek. Ukazuje se, že jednobodová množina $L = \{\boldsymbol{o}\}$ je skutečně nejmenší možný lineární prostor. Přitom $\boldsymbol{o}$ je nulový prvek z vlastnosti (7). Sčítání je definováno předpisem $\boldsymbol{o} + \boldsymbol{o} = \boldsymbol{o}$ a násobení skalárem α předpisem $\alpha \cdot \boldsymbol{o} = \boldsymbol{o}$. Takový lineární prostor nazýváme *triviální*.

1.29. Poznámka. Ukážeme, že konečná množina obsahující aspoň dva prvky nemůže být lineárním prostorem. Znamená to, že se nám pro takovou množinu L nepovede najít operace $+ : L \times L \to L$ a $\cdot : \mathbf{R} \times L \to L$ takové, aby současně splňovaly vlastnosti (1) až (7) z definice ??.

Jeden z prvků množiny L musí být nulový prvek (označme jej $\boldsymbol{o}$) a jiný prvek označme třeba $\boldsymbol{x}$. Další prvky označovat nemusíme. Uvažujme množinu $K = \{\alpha \cdot \boldsymbol{x};\ \alpha \in \mathbf{R}\}$. Protože $K \subseteq L$, je i K konečná množina. Protože reálných čísel je nekonečně mnoho, a přitom K je konečná, musejí existovat dvě různá reálná čísla $\beta \neq \gamma$ taková, že $\beta \cdot \boldsymbol{x} = \gamma \cdot \boldsymbol{x}$. Z definice lineárního prostoru ?? dostáváme:

$$\boldsymbol{o} = 0 \cdot \boldsymbol{x} = (\beta - \beta) \cdot \boldsymbol{x} = \beta \cdot \boldsymbol{x} + (-\beta) \cdot \boldsymbol{x} = \gamma \cdot \boldsymbol{x} + (-\beta) \cdot \boldsymbol{x} = (\gamma - \beta) \cdot \boldsymbol{x}.$$

Nyní máme splněny předpoklady vlastnosti (3) věty ?? (volíme $\alpha = \gamma - \beta$). Dostáváme tedy $\boldsymbol{x} = \boldsymbol{o}$. To je ale spor s předpokladem, že jsme vybrali prvek $\boldsymbol{x}$ jiný než nulový. Konečná množina obsahující aspoň dva prvky tedy nemůže být lineárním prostorem.

Existuje tedy jednobodový lineární prostor a pak dlouho nic ... a všechny ostatní lineární prostory musejí mít nekonečné množství prvků.

1.30. Příklad. Ukážeme si jeden příklad poněkud exotického lineárního prostoru. Jedná se o množinu kladných reálných čísel $\mathbf{R}^+$, na které je definováno „sčítání“ $\oplus : \mathbf{R}^+ \times \mathbf{R}^+ \to \mathbf{R}^+$ a „násobení“ reálným číslem $\odot : \mathbf{R} \times \mathbf{R}^+ \to \mathbf{R}^+$ takto: pro $x \in \mathbf{R}^+$, $y \in \mathbf{R}^+$, $\alpha \in \mathbf{R}$ je

$$x \oplus y \stackrel{\text{df}}{=} x \cdot y, \quad \alpha \odot x \stackrel{\text{df}}{=} x^\alpha,$$

kde znakem „·“ je míněno běžné násobení reálných čísel a x^α je reálná mocnina o kladném základu.

V tomto příkladě jsme se pokorně vrátili ke kroužkování nových operací sčítání a násobení skalárem, protože bychom je velmi těžko odlišovali od běžného sčítání a násobení reálných čísel. Nové sčítání vlastně definujeme jako běžné násobení a nové násobení jako běžnou mocninu.

Aby $\mathbf{R}^+$ s operacemi $\oplus$ a $\odot$ byl lineárním protorem, musí splňovat vlastnosti (1) až (7) z definice ??. Pro $x \in \mathbf{R}^+$, $y \in \mathbf{R}^+$, $z \in \mathbf{R}^+$, $\alpha \in \mathbf{R}$, $\beta \in \mathbf{R}$ je

(1) $x \oplus y = x \cdot y = y \cdot x = y \oplus x$,

(2) $(x \oplus y) \oplus z = (x \cdot y) \cdot z = x \cdot (y \cdot z) = x \oplus (y \oplus z)$,

(3) $\alpha \odot (\beta \odot x) = (\beta \odot x)^\alpha = (x^\beta)^\alpha = x^{\alpha \cdot \beta} = (\alpha\, \beta) \odot x$,

(4) $\alpha \odot (x \oplus y) = (x \oplus y)^\alpha = (x \cdot y)^\alpha = x^\alpha \cdot y^\alpha = (\alpha \odot x) \cdot (\alpha \odot y) = (\alpha \odot x) \oplus (\alpha \odot y)$,

(5) $(\alpha + \beta) \odot x = x^{\alpha+\beta} = x^\alpha \cdot x^\beta = (\alpha \odot x) \cdot (\beta \odot x) = (\alpha \odot x) \oplus (\beta \odot x)$,

(6) $1 \odot x = x^1 = x$,

(7) $0 \odot x = x^0 = 1 \in \mathbf{R}^+$.

Z poslední vlastnosti vyplývá, že nulový prvek tohoto lineárního prostoru je číslo 1. To je překvapení.

1.31. Poznámka. V definici ?? jsme za skaláry považovali reálná čísla. Nyní zkusíme nahradit v této definici všechny výskyty množiny $\mathbf{R}$ množinou komplexních čísel $\mathbf{C}$. Dostáváme pozměněnou definici:

Lineárním prostorem nazýváme každou neprázdnou množinu L, na které je definováno sčítání $+ : L \times L \to L$ a násobení komplexním číslem $\cdot : \mathbf{C} \times L \to L$ a tyto operace splňují pro každé $\boldsymbol{x} \in L$, $\boldsymbol{y} \in L$, $\boldsymbol{z} \in L$, $\alpha \in \mathbf{C}$, $\beta \in \mathbf{C}$ axiomy linearity (1) až (7) (viz definici ??). Prvky lineárního prostoru nazýváme *vektory*. Komplexnímu číslu v kontextu násobení $\cdot : \mathbf{C} \times L \to L$ říkáme *skalár*. Prvku $\boldsymbol{o} \in L$ z vlastnosti (7) říkáme *nulový prvek* nebo *nulový vektor*.

Takto definovanému lineárnímu prostoru říkáme *lineární prostor nad komplexními čísly*. Na druhé straně původní definice ?? vymezila *lineární prostor nad reálnými čísly*.

1.32. Poznámka. Když si pečlivý čtenář projde celý text této kapitoly znovu a nahradí všechny zmínky o reálných číslech zmínkami o komplexních číslech (s výjimkou příkladu ??), všechna tvrzení budou platit i v takovém případě. V našem textu si ale většinou vystačíme s lineárními prostory nad reálnými čísly. Nebude-li zde výslovně řečeno, o jaký lineární prostor se jedná, máme na mysli lineární prostor nad reálnými čísly. Přitom vesměs všechny úvahy platí i pro lineární prostory nad komplexními čísly, pokud veškeré zmínky o reálných číslech nahradíme v textu zmínkami o číslech komplexních.

1.33. Poznámka. V kapitole ?? se setkáme s dalším zobecněním lineárního prostoru. Lineární prostor nad reálnými nebo nad komplexními čísly nahradíme lineárním prostorem nad

obecným *tělesem*. Vesměs všechny vlastnosti, které dokážeme pro lineární prostory nad **R**, zůstanou v platnosti i pro lineární prostory nad obecným tělesem.

1.34. Shrnutí. V lineární algebře se pracuje s lineárními prostory /??/, což jsou množiny abstraktních „vektorů“, o nichž pouze víme, že je lze sčítat a násobit konstantou, přičemž tyto operace splňují axiomy linearity vyjmenované v definici ?? pod čísly (1) až (7).

V příkladech jsme si ukázali, že existují různé lineární prostory: prostor uspořádaných n-tic reálných čísel /??/, prostor funkcí /??/, prostor polynomů /??/, prostor nekonečných posloupností /??/, prostor orientovaných úseček /??/. Tento výčet zdaleka není úplný. Dají se sestrojit i lineární prostory s neobvyklými operacemi, které přesto splňují axiomy linearity /??/.

Nejdůležitějším příkladem je lineární prostor uspořádaných n-tic reálných čísel /??/. Vektory tohoto lineárního prostoru sčítáme po složkách a násobíme reálným číslem tak, že násobíme tímto číslem každou složku. V následujících kapitolách se s tímto lineárním prostorem ještě mnohokrát setkáme.

Podmožiny lineárních prostorů mohou se stejnými operacemi být samy lineárními prostory. V takovém případě jim říkáme podprostory /??/. Průnik podprostorů je podprostor ale sjednocení podprostorů nemusí být podprostor /??/.

2. Lineární závislost a nezávislost, lineární obal

2.1. Poznámka. Ačkoli jsme v předchozí kapitole uvedli mnoho příkladů, které měly ilustrovat definici lineárního prostoru, je možné, že smysl této definice se tím nepodařilo objasnit. Můžete se ptát, proč jsme nuceni ověřovat u různých množin, zda jsou či nejsou při definování určitých operací sčítání a násobení reálným číslem lineárními prostory. Neuvedli jsme totiž, že pokud nějaká množina je lineárním prostorem, lze na ni zkoumat mnoho dalších vlastností a zavést plno užitečných pojmů, které jsou společné všem lineárním prostorům.

Tyto vlastnosti a pojmy předpokládají pouze to, že vektory (tj. prvky nějaké blíže neurčené množiny) umíme sčítat a násobit reálným číslem, a přitom tyto operace splňují axiomy (1) až (7) z definice ??. Kdybychom tuto jednotící definici neměli, museli bychom například zvlášť zavádět pojmy lineární závislost, báze a dimenze pro množinu orientovaných úseček, zvlášť pro množinu uspořádaných n-tic a zvlášť pro množinu reálných funkcí. Až bychom třeba později zjistili, že můžeme kupříkladu matice stejné velikosti sčítat a násobit skalárem, znovu bychom pro tuto množinu byli nuceni definovat pojmy lineární závislost, báze a dimenze. Přitom k zavedení těchto pojmů je zapotřebí dokázat několik tvrzení, která bychom tak museli dokazovat pro každou konkrétní množinu zvlášť a znova. Snad každý uzná, že to je docela zbytečná práce. Je přeci jen jednodušší ověřit, že nějaká množina tvoří lineární prostor a okamžitě pro ni používat všechny další vlastnosti a pojmy, které se dozvíme v této kapitole.

2.2. Poznámka. Sčítání má podle definice ?? dva operandy. Když bychom chtěli sečíst třeba tři vektory $\boldsymbol{x}+\boldsymbol{y}+\boldsymbol{z}$, měli bychom uvést, v jakém pořadí budeme operace provádět, tj. zda provedeme $(\boldsymbol{x}+\boldsymbol{y})+\boldsymbol{z}$ nebo $\boldsymbol{x}+(\boldsymbol{y}+\boldsymbol{z})$. Vlastnost (2) definice ?? nás ale od této povinnosti osvobozuje, protože zaručuje, že oba případy povedou ke stejnému výsledku. Proto nebudeme v takovém případě nadále závorky uvádět a například pro vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ budeme jejich součet zapisovat jednoduše: $\boldsymbol{x}_1 + \boldsymbol{x}_2 + \cdots + \boldsymbol{x}_n$.

Dále budeme místo $\boldsymbol{x} + (-1) \cdot \boldsymbol{y}$ zapisovat stručně $\boldsymbol{x} - \boldsymbol{y}$. Tím vlastně máme zavedenu operaci odčítání vektorů, ačkoli tato operace není v definici ?? vůbec zmíněna.

Abychom v textu odlišili vektory (tj. prvky nějakého lineárního prostoru) od reálných čísel, budeme vektory označovat malými písmeny anglické abecedy a vždy je zvýrazníme tučně, tedy takto: $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{a}, \boldsymbol{x}_1$ atd. V ručně psaném textu se často vektory zvýrazňují zápisem šipky nad písmeno, podtržením písmene nebo i jinak.

2.3. Definice. Nechť $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou vektory (tj. prvky nějakého lineárního prostoru). *Lineární kombinací* vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ rozumíme vektor

$$\alpha_1 \cdot \boldsymbol{x}_1 + \alpha_2 \cdot \boldsymbol{x}_2 + \cdots + \alpha_n \cdot \boldsymbol{x}_n,$$

kde $\alpha_1, \alpha_2, \ldots, \alpha_n$ jsou nějaká reálná čísla. Těmto číslům říkáme *koeficienty* lineární kombinace.

2.4. Příklad. Lineární kombinací vektorů $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ může být třeba vektor $\boldsymbol{x}+\boldsymbol{y}+\boldsymbol{z}$ (všechny tři koeficienty jsou rovny jedné), nebo vektor $2\boldsymbol{x} - \boldsymbol{y} + 3{,}18\boldsymbol{z}$ (koeficienty jsou čísla 2; -1; 3,18), nebo také vektor $\alpha\,\boldsymbol{x} + \beta\,\boldsymbol{y} + \gamma\,\boldsymbol{z}$ (koeficienty $\alpha, \beta, \gamma \in \mathbf{R}$ jsme blíže neurčili).

2.5. Definice. *Triviální* lineární kombinace vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ je taková lineární kombinace, která má všechny koeficienty nulové, tj. $0\boldsymbol{x}_1 + 0\boldsymbol{x}_2 + \cdots + 0\boldsymbol{x}_n$. *Netriviální* lineární kombinace je taková lineární kombinace, která není triviální, tj. aspoň jeden její koeficient je nenulový.

2.6. Věta. Triviální lineární kombinace je vždy rovna nulovému vektoru.

Důkaz. Podle vlastnosti (7) v definici ?? je každý sčítanec v triviální lineární kombinaci roven nulovému vektoru a podle vlastnosti (1) věty ?? je i součet nulových vektorů roven nulovému vektoru.

2.7. Definice.* Skupinu vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ nazýváme *lineárně závislou*, pokud existuje netriviální lineární kombinace vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$, která je rovna nulovému vektoru. Stručně říkáme, že vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou *lineárně závislé*.

2.8. Poznámka. Pokud bychom rozvedli pojem netriviální lineární kombinace podle definic ?? a ??, můžeme říci, že vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou *lineárně závislé*, pokud existují reálná

čísla $\alpha_1, \alpha_2, \ldots, \alpha_n$ tak, že aspoň jedno z nich je nenulové, a přitom platí

$$\alpha_1 \cdot \boldsymbol{x}_1 + \alpha_2 \cdot \boldsymbol{x}_2 + \cdots + \alpha_n \cdot \boldsymbol{x}_n = \boldsymbol{o}.$$

2.9. Definice. Skupinu vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ nazýváme *lineárně nezávislou*, pokud není lineárně závislá. Stručně říkáme, že vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou *lineárně nezávislé*.

2.10. Poznámka.* Vektory jsou lineárně nezávislé, pokud (podle definic ?? a ??) neexistuje netriviální lineární kombinace těchto vektorů, která je rovna nulovému vektoru. Jinak řečeno, jedině triviální lineární kombinace je rovna nulovému vektoru. Při použití definice ?? můžeme říci, že vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou lineárně nezávislé, pokud z předpokladu $\alpha_1 \cdot \boldsymbol{x}_1 + \alpha_2 \cdot \boldsymbol{x}_2 + \cdots + \alpha_n \cdot \boldsymbol{x}_n = \boldsymbol{o}$ nutně plyne, že $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

2.11. Poznámka. Ačkoli se vesměs používá stručná formulace: „vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou lineárně závislé/nezávislé“ místo přesnějšího: „skupina vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ je lineárně závislá/nezávislá“, je potřeba si uvědomit, že stručná formulace může vést k nepochopení. Rozhodně se tím nechce říci, že jednotlivé vektory jsou lineárně závislé/nezávislé (tj. $\boldsymbol{x}_1$ je lineárně závislý/nezávislý, $\boldsymbol{x}_2$ je lineárně závislý/nezávislý atd.), ale jedná se vždy o vlastnost celé skupiny vektorů jako celku.

Pojem lineární závislosti a nezávislosti vektorů má v lineární algebře zásadní důležitost. Závislost vektorů je možná názornější z pohledu následující věty ??, ovšem při ověřování

lineární závislosti abstraktních vektorů je často definice ?? použitelnější. Má proto smysl definicím ?? a ?? věnovat náležitou pozornost.

2.12. Příklad. Uvažujme lineární prostor $\mathbf{R}^3$ (viz příklad ??, $n = 3$). Jsou dány tři vektory z $\mathbf{R}^3$:

$$\boldsymbol{x} = (1, 2, 3), \quad \boldsymbol{y} = (1, 0, 2), \quad \boldsymbol{z} = (-1, 4, 0).$$

Zjistíme z definice, zda jsou vektory $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ lineárně závislé či nezávislé. Podle poznámek ?? a ?? stačí zjistit, jaké mohou být koeficienty α, β, γ, pokud položíme

$$\alpha\,\boldsymbol{x} + \beta\,\boldsymbol{y} + \gamma\,\boldsymbol{z} = \boldsymbol{o}.$$

Dosazením do této rovnice dostáváme

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

Zde jsme využili toho, že nulový vektor v $\mathbf{R}^3$ je roven trojici $(0, 0, 0)$. Dále podle definice sčítání a násobení skalárem na $\mathbf{R}^3$ dostáváme

$$(\alpha + \beta - \gamma, 2\,\alpha + 4\,\gamma, 3\,\alpha + 2\,\beta) = (0, 0, 0).$$

Dvě uspořádané trojice se rovnají, pokud se rovnají jejich odpovídající složky. Musí tedy platit tyto rovnice:

$$\begin{aligned} \alpha + \beta - \gamma &= 0, \\ 2\,\alpha + 4\,\gamma &= 0, \\ 3\,\alpha + 2\,\beta &= 0. \end{aligned}$$

Tato soustava má nekonečně mnoho řešení (zkuste si to ověřit třeba Gaussovou eliminační metodou). Mezi těmito řešeními je jediné triviální, všechna ostatní jsou netriviální. Příkladem takového netriviálního řešení může být třeba $\alpha = 2$, $\beta = -3$, $\gamma = -1$, takže

$$2\,(1,2,3) - 3\,(1,0,2) - 1\,(-1,4,0) = (0,0,0).$$

Existuje tedy netriviální lineární kombinace vektorů $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$, která je rovna nulovému vektoru, což podle definice ?? znamená, že vektory $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ jsou lineárně závislé.

2.13. Příklad. V lineárním prostoru $\mathbf{R}^3$ jsou dány tři vektory z $\mathbf{R}^3$:

$$\boldsymbol{x} = (1,2,3), \quad \boldsymbol{y} = (1,0,2), \quad \boldsymbol{z} = (-2,1,0).$$

Zjistíme z definice, zda jsou vektory $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ lineárně závislé či nezávislé. Podle poznámek ?? a ?? stačí zjistit, jaké mohou být koeficienty α, β, γ, pokud položíme $\alpha\,\boldsymbol{x} + \beta\,\boldsymbol{y} + \gamma\,\boldsymbol{z} = \boldsymbol{o}$. Dosazením do této rovnice dostáváme

$$\begin{aligned} \alpha\,(1,2,3) + \beta\,(1,0,2) + \gamma\,(-2,1,0) &= (0,0,0), \\ (\alpha + \beta - 2\,\gamma, 2\,\alpha + \gamma, 3\,\alpha + 2\,\beta) &= (0,0,0). \end{aligned}$$

Dvě uspořádané trojice se rovnají, pokud se rovnají jejich odpovídající složky. Musí tedy platit tyto rovnice:

$$\begin{aligned} \alpha + \beta - 2\gamma &= 0, \\ 2\alpha + \gamma &= 0, \\ 3\alpha + 2\beta &= 0. \end{aligned}$$

Tato soustava má jediné řešení $\alpha = 0, \beta = 0, \gamma = 0$ (zkuste si to ověřit třeba Gaussovou eliminační metodou). Vidíme tedy, že jedině triviální lineární kombinace vektorů $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ je rovna nulovému vektoru, což podle definice ?? znamená, že vektory $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ jsou lineárně nezávislé.

2.14. Příklad. Uvažujme lineární prostor všech reálných funkcí definovaných na $\mathbf{R}$ a v něm tři funkce f, g, h, které jsou zadané těmito vzorci:

$$f(x) = \sin(x), \quad g(x) = \cos(x), \quad h(x) = 4 \quad \forall x \in \mathbf{R}.$$

Ověříme, zda jsou tyto tři funkce lineárně nezávislé či závislé. Položíme jejich lineární kombinaci rovnu nulové funkci:

$$\alpha \cdot \sin(x) + \beta \cdot \cos(x) + \gamma \cdot 4 = 0 \quad \forall x \in \mathbf{R} \tag{2.1}$$

a zjistíme, jakých hodnot mohou nabývat koeficienty α, β, γ. Tato rovnost má být splněna pro všechna $x \in \mathbf{R}$. Je možné, že při volbě tří hodnot $x \in \mathbf{R}$ už vynutíme trivialitu lineární

kombinace v (2.1). Zkusme štěstí například pro $x \in \{0, \frac{\pi}{2}, \pi\}$. V rovnici (2.1) se tedy omezíme na

$$\alpha \cdot \sin(x) + \beta \cdot \cos(x) + \gamma \cdot 4 = 0 \quad \text{pro } x \in \left\{0, \frac{\pi}{2}, \pi\right\}. \tag{2.2}$$

Po dosazení hodnot x dostáváme tři rovnice:

$$\begin{aligned} 0\,\alpha + \;\; \beta + 4\,\gamma &= 0, \\ \alpha + 0\,\beta + 4\,\gamma &= 0, \\ 0\,\alpha - \;\; \beta + 4\,\gamma &= 0. \end{aligned}$$

Tato soustava má jediné řešení $\alpha = 0$, $\beta = 0$, $\gamma = 0$ (zkuste si to ověřit třeba Gaussovou eliminační metodou). Takže pokus se zdařil. Z rovnice (2.1) plyne (2.2) a z ní pak $\alpha = 0$, $\beta = 0$, $\gamma = 0$. To podle definice znamená, že vektory f, g, h jsou lineárně nezávislé.

2.15. Příklad. Uvažujme lineární prostor všech reálných funkcí definovaných na $\mathbf{R}$ a v něm tři funkce f, g, h, které jsou zadané těmito vzorci:

$$f(x) = \sin^2(x), \quad g(x) = 3\,\cos^2(x), \quad h(x) = 4 \quad \forall x \in \mathbf{R}.$$

Ověříme, zda jsou tyto tři funkce lineárně nezávislé či závislé. Položíme jejich lineární kombinaci rovnu nulové funkci:

$$\alpha \cdot \sin^2(x) + \beta \cdot 3\,\cos^2(x) + \gamma \cdot 4 = 0 \quad \forall x \in \mathbf{R} \tag{2.3}$$

a zjistíme, jakých hodnot mohou nabývat koeficienty α, β, γ. Jako v příkladu ?? zkusíme volit nějaké tři hodnoty x. Po dosazení $x = 0$, $x = \pi/2$ a $x = \pi$ dostáváme soustavu

$$\begin{array}{rrcl} & 3\,\beta + 4\,\gamma & = & 0, \\ \alpha & + 4\,\gamma & = & 0, \\ & 3\,\beta + 4\,\gamma & = & 0. \end{array}$$

Vidíme, že jedna rovnice je zde napsaná dvakrát, takže zbývají dvě rovnice o třech neznámých. Taková soustava rovnic má nekonečně mnoho řešení, jedním z nich je například $\alpha = 12$, $\beta = 4$, $\gamma = -3$. To nám ale k závěru o lineární závislosti funkcí nestačí, protože my musíme najít netriviální kombinaci rovnou nule pro všechna $x \in \mathbf{R}$, nikoli jen pro tři vyvolené hodnoty. Výsledek ale napovídá, jaké by mohly být koeficienty hledané netriviální lineární kombinace:

$$12 \cdot \sin^2(x) + 4 \cdot 3\,\cos^2(x) - 3 \cdot 4 = 12\,(\sin^2(x) + \cos^2(x)) - 12 = 0 \quad \forall\, x \in \mathbf{R}.$$

Zde jsme využili vzorce $\sin^2(x) + \cos^2(x) = 1$ pro všecha $x \in \mathbf{R}$. Našli jsme tedy netriviální lineární kombinaci, která je rovna nulové funkci na celém definičním oboru, a proto jsou funkce f, g, h lineárně závislé.

2.16. Poznámka. Při vyšetřování lineární nezávislosti funkcí můžeme též využít derivací. Třeba rovnost (2.1) má platit pro všechna $x \in \mathbf{R}$ a tím pádem pro všechny derivace v libovolném bodě. Třeba v nule. Pro $x = 0$ je $\beta + 4\gamma = 0$, po zderivování máme $\alpha \cos(x) - \beta \sin(x) = 0$

a dosazením $x = 0$ dostaneme druhou rovnost $\alpha = 0$. Ještě jednou zderivjeme a dosadíme $x = 0$, máme $\beta = 0$. Z první rovnosti plyne, že tedy musí $\alpha = 0$. Všechny koeficienty musejí být nulové, takže vektory f, g, h z příkladu ?? jsou lineárně nezávislé.

Na druhé straně postupným derivováním rovnosti (2.3) z příkladu ?? a dosazením $x = 0$ dostáváme rovnice: $3\beta + 4\gamma = 0$, $0 = 0$, $\alpha - 3\beta = 0$, $0 = 0$, $0 = 0$, atd. (zkuste si sami zderivovat). Takže máme jen dvě nenulové rovnice o třech neznámých, tedy α, β, γ mohou být nenulové. Tento postup nám tedy nedává záruku nezávislosti funkcí f, g, h z příkladu ??.

2.17. Příklad. Nechť $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$ jsou prvky nějakého (blíže nespecifikovaného) lineárního prostoru. Předpokládejme, že jsou lineárně nezávislé. Úkolem je zjistit, pro které $a \in \mathbf{R}$ jsou vektory

$$\boldsymbol{x} = 2\,\boldsymbol{u} - \boldsymbol{v}, \quad \boldsymbol{y} = \boldsymbol{u} + 3\,\boldsymbol{v} - 2\,\boldsymbol{w}, \quad \boldsymbol{z} = \boldsymbol{v} + a\,\boldsymbol{w}$$

lineárně závislé.

Položíme tedy lineární kombinaci vektorů $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ rovnu nulovému vektoru a budeme zjišťovat, jaké musí být koeficienty α, β, γ:

$$\alpha\,\boldsymbol{x} + \beta\,\boldsymbol{y} + \gamma\,\boldsymbol{z} = \boldsymbol{o}.$$

Dosadíme:

$$\alpha\,(2\,\boldsymbol{u} - \boldsymbol{v}) + \beta\,(\boldsymbol{u} + 3\,\boldsymbol{v} - 2\,\boldsymbol{w}) + \gamma\,(\boldsymbol{v} + a\,\boldsymbol{w}) = \boldsymbol{o}$$

a po úpravách dostáváme

$$(2\,\alpha+\beta)\,\boldsymbol{u}+(-\alpha+3\,\beta+\gamma)\,\boldsymbol{v}+(-2\,\beta+a\,\gamma)\,\boldsymbol{w}=\boldsymbol{o}.$$

Protože podle předpokladů jsou vektory $\boldsymbol{u},\boldsymbol{v},\boldsymbol{w}$ lineárně nezávislé, musí být tato lineární kombinace jedině triviální, tj. všechny koeficienty jsou nulové:

$$\begin{aligned} 2\,\alpha+\ \beta\ &=0,\\ -\alpha+3\,\beta+\ \gamma\ &=0,\\ -2\,\beta+a\,\gamma\ &=0. \end{aligned}$$

Například pomocí Gaussovy eliminační metody se můžeme přesvědčit, že soustava má jediné řešení $\alpha=0$, $\beta=0$, $\gamma=0$ pro $7a+4\neq 0$. V takovém případě budou vektory $\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}$ lineárně nezávislé. Jestliže naopak $7a+4=0$, má soustava nekonečně mnoho řešení, mezi kterými se jistě najde i netriviální řešení. Vektory $\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}$ jsou tedy lineárně závislé pro $a=-4/7$.

2.18. Věta.* Nechť $n\geq 2$. Vektory $\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_n$ jsou lineárně závislé právě tehdy, když existuje index $r\in\{1,\ldots,n\}$ takový, že vektor $\boldsymbol{x}_r$ je roven lineární kombinaci ostatních vektorů.

Důkaz. Věty formulované ve tvaru ekvivalence (výrok A platí právě tehdy, když platí výrok B) se obvykle dokazují ve dvou krocích. Nejprve dokážeme, že z A plyne B a pak dokážeme, že z B plyne A.

Dokazujme tedy nejprve, že z lineární závislosti vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ plyne existence indexu r výše uvedené vlastnosti. Z definice lineární závislosti víme, že existuje netriviální lineární kombinace rovna nulovému vektoru, tj.

$$\alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_n \boldsymbol{x}_n = \sum_{i=1}^{n} \alpha_i \boldsymbol{x}_i = \boldsymbol{o}, \tag{2.4}$$

a přitom aspoň jeden koeficient lineární kombinace je nenulový. Existuje tedy $r \in \{1, \ldots, n\}$ takové, že $\alpha_r \neq 0$. Přičteme nyní vektor $-\alpha_r \boldsymbol{x}_r$ k oběma stranám rovnice (2.4)

$$\sum_{\substack{i=1 \\ i \neq r}}^{n} \alpha_i \boldsymbol{x}_i = -\alpha_r \boldsymbol{x}_r.$$

Po vynásobení obou stran rovnice koeficientem $-1/\alpha_r$ dostáváme

$$\sum_{\substack{i=1 \\ i \neq r}}^{n} \frac{\alpha_i}{-\alpha_r} \boldsymbol{x}_i = \boldsymbol{x}_r.$$

Vektor $\boldsymbol{x}_r$ je tedy roven lineární kombinaci ostatních vektorů.

V druhé části důkazu předpokládáme existenci koeficientu r takového, že vektor $\boldsymbol{x}_r$ je roven lineární kombinaci ostatních vektorů. Dokážeme lineární závislost vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$. Pro nějaké $r \in \{1, \ldots, n\}$ tedy platí

$$\boldsymbol{x}_r = \sum_{\substack{i=1 \\ i \neq r}}^{n} \beta_i \, \boldsymbol{x}_i.$$

Přičteme-li k oběma stranám této rovnice vektor $-\boldsymbol{x}_r$, dostáváme

$$\sum_{\substack{i=1 \\ i \neq r}}^{n} \beta_i \, \boldsymbol{x}_i + (-1) \cdot \boldsymbol{x}_r = \boldsymbol{o},$$

což je netriviální lineární kombinace vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ (její r-tý koeficient je jistě nenulový), která je rovna nulovému vektoru.

2.19. Poznámka. Věta ?? se dá přeformulovat též takto: vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou lineárně nezávislé právě tehdy, když žádný z vektorů $\boldsymbol{x}_i$, $i \in \{1, \ldots, n\}$, není lineární kombinací ostatních vektorů.

2.20. Věta. Nechť $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou prvky nějakého lineárního prostoru L. Pak platí:
(1) Lineární závislost či nezávislost vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ se nezmění při změně pořadí těchto vektorů.
(2) Jestliže se mezi $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ vyskytuje nulový vektor, pak jsou tyto vektory lineárně závislé.
(3) Jestliže se ve skupině vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ některý vektor vyskytuje aspoň dvakrát, je tato skupina vektorů lineárně závislá.
(4) Jestliže jsou vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ lineárně závislé a $\boldsymbol{x}_{n+1} \in L$, pak jsou i vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n, \boldsymbol{x}_{n+1}$ lineárně závislé.
(5) Jestliže jsou vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ lineárně nezávislé, pak jsou i vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{n-1}$ lineárně nezávislé.
(6) Samotný vektor $\boldsymbol{x}_1$ (chápaný ovšem jako skupina vektorů o jednom prvku) je lineárně nezávislý právě tehdy, když je nenulový.
(7) Dva vektory jsou lineárně závislé právě tehdy, když jeden je násobkem druhého.

Důkaz. (1) Lineární kombinace vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ nezávisí na jejich pořadí, protože sčítání vektorů je podle definice ?? komutativní.

(2) Vzhledem k vlastnosti (1) stačí bez újmy na obecnosti předpokládat, že $\boldsymbol{o} = \boldsymbol{x}_1$. Pak platí:

$$1 \cdot \boldsymbol{o} + 0 \cdot \boldsymbol{x}_2 + 0 \cdot \boldsymbol{x}_3 + \cdots + 0 \cdot \boldsymbol{x}_n = \boldsymbol{o},$$

což je netriviální lineární kombinace rovna nulovému vektoru.

(3) Vzhledem k vlastnosti (1) stačí bez újmy na obecnosti předpokládat, že $\boldsymbol{x}_1 = \boldsymbol{x}_2$. Pak platí:

$$1 \cdot \boldsymbol{x}_1 + (-1) \cdot \boldsymbol{x}_2 + 0 \cdot \boldsymbol{x}_3 + \cdots + 0 \cdot \boldsymbol{x}_n = (1-1) \cdot \boldsymbol{x}_1 = \boldsymbol{o},$$

což je netriviální lineární kombinace rovna nulovému vektoru.

(4) Podle předpokladu existuje netriviální lineární kombinace $\alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_n \boldsymbol{x}_n$ rovna nulovému vektoru. Potom platí

$$\alpha_1 \boldsymbol{x}_1 + \cdots + \alpha_n \boldsymbol{x}_n + 0 \cdot \boldsymbol{x}_{n+1} = \boldsymbol{o},$$

což je netriviální lineární kombinace vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n, \boldsymbol{x}_{n+1}$ rovna nulovému vektoru.

(5) Dokážeme to sporem. Budeme předpokládat negaci tvrzení věty (tj. že vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{n-1}$ jsou lineárně závislé). Pak ale podle vlastnosti (4) musejí být lineárně závislé i vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$, což je spor s předpokladem, že tyto vektory jsou lineárně nezávislé.

(6) Je-li $\boldsymbol{x}_1 = \boldsymbol{o}$, pak je $\boldsymbol{x}_1$ podle vlastnosti (2) lineárně závislý. Předpokládejme nyní $\boldsymbol{x}_1 \neq \boldsymbol{o}$ a položme

$$\alpha \boldsymbol{x}_1 = \boldsymbol{o}.$$

Kdyby bylo $\alpha \neq 0$, pak dostáváme spor s vlastností (3) věty ??. Musí tedy být $\alpha = 0$. To znamená, že pouze triviální lineární kombinace je rovna nulovému vektoru, takže vektor $\boldsymbol{x}_1$ je lineárně nezávislý.

(7) Tvrzení je shodné s větou ?? pro $n = 2$.

2.21. Poznámka. Vlastnost (4) předchozí věty nelze „obrátit“. Přesněji: z lineární závislosti vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ neplyne nic o lineární závislosti či nezávislosti vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{n-1}$. Může se třeba stát, že vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{n-1}$ jsou lineárně nezávislé a lineární závislost vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ je způsobena tím, že vektor $\boldsymbol{x}_n$ je nulový. Může se ale také stát, že vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{n-1}$ zůstávají lineárně závislé.

Vlastnost (5) předchozí věty nelze „obrátit“. Přesněji: z lineární nezávislosti vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ neplyne nic o lineární závislosti či nezávislosti vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{n+1}$. Vektor $\boldsymbol{x}_{n+1}$ totiž může být nulový, ale také může být takový, že vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{n+1}$ zůstávají lineárně nezávislé.

2.22. Příklad. Nechť $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m$ jsou vektory z lineárního prostoru $\mathbf{R}^n$. Ukážeme, že pokud $m > n$, jsou nutně tyto vektory lineárně závislé.

Podle definice lineární závislosti hledejme netriviální lineární kombinaci, pro kterou

$$\alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_m \boldsymbol{x}_m = \boldsymbol{o}.$$

Rozepsáním tohoto požadavku do složek dostáváme n rovnic o m neznámých. Protože pravé strany rovnic jsou nulové, soustava má určitě aspoň triviální řešení. Protože je v soustavě více neznámých než rovnic existuje nekonečně mnoho řešení této soustavy. Mezi těmito řešeními je jen jediné triviální a všechna ostatní jsou netriviální.

Poznamenejme, že příklad ukazuje důležitou vlastnost lineárních prostorů $\mathbf{R}^n$: všechny lineárně nezávislé skupiny vektorů mají počet vektorů menší nebo roven n. Podobné tvrzení pro libovolné lineární prostory vyslovíme ve větě ??.

2.23. Příklad. Uvažujme lineární prostor U_O všech orientovaných úseček z příkladu ??.

(1) Leží-li dvě úsečky $\boldsymbol{u}, \boldsymbol{v} \in U_O$ ve stejné přímce, pak jsou lineárně závislé, protože jedna je násobkem druhé. Neleží-li úsečky $\boldsymbol{u}, \boldsymbol{v}$ ve společné přímce, pak jsou lineárně nezávislé.

(2) Nechť $\boldsymbol{u}, \boldsymbol{v} \in U_O$ jsou lineárně nezávislé. Pak množina všech lineárních kombinací $\alpha\,\boldsymbol{u} + \beta\,\boldsymbol{v}$ vyplňuje množinu všech úseček, které mají koncový bod v rovině určené úsečkami $\boldsymbol{u}, \boldsymbol{v}$.

Abychom to dokázali, potřebujeme určitou představivost a zkušenosti s euklidovskou geometrií. Připomeňme, že O značí společný počátek všech orientovaných úseček našeho lineárního prostoru. Zvolme nyní libovolnou orientovanou úsečku $\boldsymbol{x}$ s počátkem v O, která leží v rovině určené úsečkami $\boldsymbol{u}, \boldsymbol{v}$. Ukážeme, že existují $\alpha, \beta \in \mathbf{R}$ tak, že $\boldsymbol{x} = \alpha\,\boldsymbol{u} + \beta\,\boldsymbol{v}$. Leží-li $\boldsymbol{x}$ na společné přímce s úsečkou $\boldsymbol{u}$ nebo na přímce společné s úsečkou $\boldsymbol{v}$, pak je $\boldsymbol{x}$ násobkem této úsečky a druhý koeficient hledané lineární kombinace je nulový. Nechť tedy $\boldsymbol{x}$ neleží na žádné z těchto přímek. Nakreslíme na tyto přímky měřítka, jako v příkladu ??. Koncový bod úsečky $\boldsymbol{x}$ označme X. Veďme bodem X rovnoběžky s oběma měřítky. Hodnota na měřítku podél vektoru $\boldsymbol{u}$ v místě průsečíku rovnoběžky s měřítkem je číslo α. Číslo β je pak v místě průsečíku druhé rovnoběžky na druhém měřítku. Z definice sčítání orientovaných úseček pomocí rovnoběžníka vidíme, že $\boldsymbol{x} = \alpha\,\boldsymbol{u} + \beta\,\boldsymbol{v}$. Udělejte si náčrtek.

(3) Leží-li tři usečky $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in U_O$ ve společné rovině, pak jsou lineárně závislé, protože z (2) plyne, že jedna z nich je lineární kombinací ostatních. Dále použijeme větu ??.

(4) Pokud $\boldsymbol{u}$ a $\boldsymbol{v} \in U_O$ jsou lineárně nezávislé a $\boldsymbol{w}$ leží mimo rovinu danou úsečkami $\boldsymbol{u}, \boldsymbol{v}$, pak jsou $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$ lineárně nezávislé.

(5) Nechť $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in U_O$ jsou lineárně nezávislé. Pak množina všech lineárních kombinací

$$\alpha\,\boldsymbol{u} + \beta\,\boldsymbol{v} + \gamma\,\boldsymbol{w}$$

vyplňuje celý lineární prostor U_O.

Abychom to dokázali, potřebujeme opět určitou představivost. Nechť ϱ je rovina určená úsečkami $\boldsymbol{u}$ a $\boldsymbol{v}$. Ukážeme, že pro libovolnou orientovanou úsečku $\boldsymbol{x}$ s počátkem v O existují reálná čísla α, β, γ taková, že $\boldsymbol{x} = \alpha\,\boldsymbol{u} + \beta\,\boldsymbol{v} + \gamma\,\boldsymbol{w}$. Leží-li $\boldsymbol{x}$ v rovině ϱ, položíme $\gamma = 0$ a dále využijeme výsledku z (2). Nechť tedy $\boldsymbol{x}$ neleží v rovině ϱ. Označme X koncový bod úsečky $\boldsymbol{x}$. Veďme bodem X rovnoběžku s úsečkou $\boldsymbol{w}$. Ta nutně protne rovinu ϱ v nějakém bodě P. Podle (2) existují $\alpha, \beta \in \mathbf{R}$ takové, že $\overrightarrow{OP} = \alpha\,\boldsymbol{u} + \beta\,\boldsymbol{v}$. V rovině určené vektory $\boldsymbol{x}$ a $\boldsymbol{w}$ veďme rovnoběžku s vektorem $\overrightarrow{OP}$. Ta protne měřítko procházející vektorem $\boldsymbol{w}$ v místě s hodnotou γ. Je $\boldsymbol{x} = \overrightarrow{OP} + \gamma\,\boldsymbol{w} = \alpha\,\boldsymbol{u} + \beta\,\boldsymbol{v} + \gamma\,\boldsymbol{w}$.

2.24. Poznámka. Až dosud jsme pracovali s pojmem lineární závislost či nezávislost konečných *skupin* vektorů. Skupina, na rozdíl od množiny, může obsahovat stejné prvky a je vždy konečná. V následující definici rozšíříme pojem lineární závislost či nezávislost na konečné i

nekonečné *množiny* vektorů. Definice lineární závislosti se může jevit poněkud nepřímočará. Je to tím, že množiny vektorů mohou být nekonečné, a přitom nelze sestavovat nekonečné lineární kombinace vektorů.

2.25. Definice.* Nechť L je lineární prostor a nechť $M \subseteq L$ je neprázdná množina vektorů. Množina M je *lineárně závislá*, pokud existuje konečně mnoho různých vektorů z M, které jsou lineárně závislé. Množina M je *lineárně nezávislá*, pokud není lineárně závislá. Tedy pokud neexistuje žádná její konečná lineárně závislá podmnožina.

Prázdnou množinu považujeme vždy za lineárně nezávislou.

2.26. Poznámka.* Uvědomíme si podrobněji základní vlastnost lineárně závislých množin. Množina vektorů M je lineárně závislá, právě když existuje konečně mnoho vektorů z této množiny, které jsou lineárně závislé. Podle věty ?? to znamená, že existuje jeden vektor $\boldsymbol{z} \in M$, který je roven lineární kombinaci konečně mnoha jiných vektorů z této množiny.

2.27. Poznámka. Uvědomíme si podrobněji základní vlastnost lineárně nezávislých množin.

Neprázdná konečná množina vektorů $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$ je lineárně nezávislá, právě když jsou vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ lineárně nezávislé (odkazujeme na definici ??).

Z opakovaného použití vlastnosti (5) věty ?? (nebo z věty ??) totiž plyne, že je-li konečná množina vektorů K lineárně nezávislá, pak všechny její podmnožiny $K' \subseteq K$ jsou lineárně nezávislé.

Nekonečná množina vektorů $M \subseteq L$ je podle definice ?? lineárně nezávislá, pokud všechny její konečné podmnožiny $K \subseteq M$ jsou lineárně nezávislé.

Nechť nekonečná množina $M \subseteq L$ je lineárně nezávislá a $M' \subseteq M$ je její nekonečná podmnožina. Pak M' musí být také lineárně nezávislá, protože všechny její konečné podmnožiny jsou též konečnými podmnožinami množiny M. Takže dostáváme následující větu, ve které už nerozlišujeme mezi konečnými a nekonečnými (pod)množinami:

2.28. Věta.* Je-li množina vektorů M v lineárním prostoru L je lineárně nezávislá, pak každá její podmnožina je lineárně nezávislá.

Důkaz. Viz poznámku ??.

2.29. Poznámka. Větu ?? nelze obrátit ve smyslu, že pokud každá množina $N \subset M$, $N \neq M$, je lineárně nezávislá, pak je M lineárně nezávislá. Toto neplatí. Představme si tři orientované úsečky lineárního prostoru U_O (viz příklad ??) ležící ve společné rovině, ale žádné dva neleží na společné přímce. Množinu těchto tří vektorů označme M. Pak každá podmnožina N množiny M, $N \neq M$, je lineárně nezávislá, ale M je lineárně závislá.

2.30. Příklad. Nechť $M = \{1, x, x^2, x^3, \ldots\}$ je nekonečná podmnožina lineárního prostoru všech polynomů P. Ukážeme, že M je lineárně nezávislá.

Podle definice ?? a poznámky ?? stačí ukázat, že každá konečná podmnožina polynomů

$$K = \{x^{k_1}, x^{k_2}, \dots, x^{k_n}\}, \quad n \in \mathbf{N}, \quad k_i \in \mathbf{N} \cup \{0\} \text{ pro } i \in \{1, 2, \dots, n\}, \quad k_1 < k_2 < \dots < k_n$$

je lineárně nezávislá. Položme tedy lineární kombinaci prvků množiny K rovnu nulovému polynomu:

$$\alpha_1 x^{k_1} + \alpha_2 x^{k_2} + \dots + \alpha_n x^{k_n} = 0 \quad \forall x \in \mathbf{R}$$

a ptejme se, co z toho plyne pro koeficienty $\alpha_1, \dots, \alpha_n$. Protože $k_1 < k_2 < \dots < k_n$, odpovídají čísla $\alpha_1, \dots, \alpha_n$ vybraným koeficientům polynomu. Nulový polynom je ovšem pouze takový polynom, který má všechny koeficienty nulové . Takže všechna čísla $\alpha_1, \dots, \alpha_n$ musejí být rovna nule. Nulovému polynomu se tedy rovná pouze triviální lineární kombinace, takže množina K je lineárně nezávislá.

2.31. Definice.* Nechť L je lineární prostor. *Lineární obal* skupiny vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_n$ značíme $\langle \boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_n \rangle$ a je to množina všech lineárních kombinací vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_n$.

Nechť dále $M \subseteq L$ je neprázdná množina vektorů. *Lineární obal* množiny vektorů M je množina všech konečných lineárních kombinací vektorů z M. Lineární obal množiny M značíme symbolem $\langle M \rangle$.

Lineární obal prázdné množiny definujeme jako jednoprvkovou množinu obsahující nulový vektor.

2.32. Poznámka. Podle definice ?? je

$$\langle \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \rangle = \{\alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_n \boldsymbol{x}_n;\ \alpha_1 \in \mathbf{R}, \alpha_2 \in \mathbf{R}, \ldots, \alpha_n \in \mathbf{R}\}.$$

Je zřejmé, že $\langle \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \rangle = \langle \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\} \rangle$. Na pravé straně této rovnosti sice jsou přidány i lineární kombinace všech konečných podmnožin množiny $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$, ale ty se dají zapsat jako lineární kombinace všech vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$. Stačí totiž vektory mimo konečný výběr násobit nulou.

2.33. Poznámka. V lineární algebře se nikdy nepracuje s nekonečným součtem násobků vektorů, všechny lineární kombinace musejí být vždy tvořeny konečným součtem. Definice ?? připouští, že množina vektorů M může být nekonečná, ale i v takovém případě lineární obal sestavujeme z *konečných* součtů, tj. vybíráme konečné podmnožiny vektorů z M, ze kterých sestavujeme lineární kombinace. Samozřejmě, že takových výběrů může být nekonečně mnoho a z každého konečného výběru vektorů můžeme sestavit nekonečně mnoho lineárních kombinací. Takže lineární obal je nekonečná množina (s jedinou výjimkou: lineární obal nulového vektoru nebo prázdné množiny).

2.34. Příklad. Uvažujme lineární prostor $\mathbf{R}^3$. Najdeme lineární obal vektorů $x = (1, 2, 3)$, $y = (2, -1, 0)$. Podle poznámky ?? je

$$\langle (1,2,3), (2,-1,0) \rangle = \{\alpha\,(1,2,3) + \beta\,(2,-1,0);\ \alpha \in \mathbf{R}, \beta \in \mathbf{R}\} = \{(\alpha+2\beta, 2\alpha-\beta, 3\alpha);\ \alpha \in \mathbf{R}, \beta \in$$

2.35. Příklad. Jsou dány $\boldsymbol{x} = (1, 2, 3)$, $\boldsymbol{y} = (1, 0, 2)$, $\boldsymbol{z} = (-2, 1, 0)$. Ukážeme, že $\langle \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \rangle = \mathbf{R}^3$.

Množina lineárních kombinací prvků nějakého lineárního prostoru L je vždy podmnožinou L. Jde tedy pouze o to ukázat, že $\mathbf{R}^3 \subseteq \langle \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \rangle$. Volme libovolný vektor $(a, b, c) \in \mathbf{R}^3$. Ukážeme, že (a, b, c) leží v $\langle \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \rangle$. K tomu je potřeba najít lineární kombinaci vektorů $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$, která je rovna vektoru (a, b, c). Hledejme tedy koeficienty α, β, γ, pro které platí

$$(a, b, c) = \alpha\,(1, 2, 3) + \beta\,(1, 0, 2) + \gamma\,(-2, 1, 0).$$

Po úpravě a porovnání jednotlivých složek dostáváme soustavu

$$\begin{aligned} \alpha + \beta - 2\gamma &= a, \\ 2\alpha + \gamma &= b, \\ 3\alpha + 2\beta &= c. \end{aligned}$$

Například Gaussovou eliminační metodou zjistíme, že soustava má řešení pro všechna $a, b, c \in \mathbf{R}$. Proto $(a, b, c) \in \langle \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \rangle$.

2.36. Poznámka. Zamysleme se nad tím, co to znamená, že $\boldsymbol{z} \in \langle M \rangle$. Vektor $\boldsymbol{z}$ je lineární kombinací nějakého konečného výběru vektorů z množiny M.

Vidíme tedy, že $\boldsymbol{z} \in \langle M \rangle$ právě tehdy, když existuje konečně mnoho vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \in M$ a existují reálná čísla $\alpha_1, \alpha_2, \ldots, \alpha_n$ taková, že

$$\boldsymbol{z} = \alpha_1\,\boldsymbol{x}_1 + \alpha_2\,\boldsymbol{x}_2 + \cdots + \alpha_n\,\boldsymbol{x}_n. \tag{2.5}$$

2.37. Věta.* Nechť L je lineární prostor a $M \subseteq L$. Pak platí:

(1) $M \subseteq \langle M \rangle$.
(2) Je-li $N \subseteq M$, pak $\langle N \rangle \subseteq \langle M \rangle$.
(3) $\langle M \rangle = \langle \langle M \rangle \rangle$.
(4) Je-li $\boldsymbol{z} \in \langle M \rangle$, pak $\langle M \rangle = \langle M \cup \{\boldsymbol{z}\} \rangle$.

Důkaz. (1) Stačí ukázat, že pokud $\boldsymbol{z} \in M$ pak $\boldsymbol{z} \in \langle M \rangle$. Platí $\boldsymbol{z} = 1 \cdot \boldsymbol{z}$, takže pro $\boldsymbol{z}$ existuje konečně mnoho prvků z M (jmenovitě prvek $\boldsymbol{z}$ samotný) tak, že $\boldsymbol{z}$ je lineární kombinací těchto prvků. To podle poznámky ?? znamená, že $\boldsymbol{z} \in \langle M \rangle$.

(2) Nechť $\boldsymbol{z} \in \langle N \rangle$, tj. předpokládáme, že $\boldsymbol{z}$ lze zapsat jako lineární kombinaci konečně mnoha prvků z N. Protože tyto prvky leží i v M, můžeme říci, že $\boldsymbol{z}$ lze zapsat jako lineární kombinaci konečně mnoha prvků z M. To podle poznámky ?? znamená, že $\boldsymbol{z} \in \langle M \rangle$.

(3) Vzhledem k (1) a (2) je $\langle M \rangle \subseteq \langle \langle M \rangle \rangle$. Stačí tedy ukázat, že $\langle \langle M \rangle \rangle \subseteq \langle M \rangle$. Nechť $\boldsymbol{z} \in \langle \langle M \rangle \rangle$, ukážeme že $\boldsymbol{z} \in \langle M \rangle$. Protože $\boldsymbol{z} \in \langle \langle M \rangle \rangle$, existují vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \in \langle M \rangle$ takové, že platí (2.5). Pro každé $i \in \{1, \ldots, n\}$ je $\boldsymbol{x}_i \in \langle M \rangle$, tj. existuje konečně mnoho vektorů $\boldsymbol{y}_{i,1}, \ldots, \boldsymbol{y}_{i,k_i} \in M$ takových, že

$$\boldsymbol{x}_i = \beta_{i,1}\, \boldsymbol{y}_{i,1} + \cdots + \beta_{i,k_i}\, \boldsymbol{y}_{i,k_i}.$$

Dosazením těchto rovnic do (2.5) a roznásobením dostáváme výsledek, že $\boldsymbol{z}$ je lineární kombinací konečně mnoha vektorů $\boldsymbol{y}_{i,j} \in M$, $i \in \{1, \ldots, n\}, j \in \{1, \ldots, k_i\}$. To znamená, že $\boldsymbol{z} \in \langle M \rangle$.

(4) Protože $M \subseteq M \cup \{\boldsymbol{z}\}$, je podle (2) $\langle M \rangle \subseteq \langle M \cup \{\boldsymbol{z}\} \rangle$. Protože $\boldsymbol{z} \in \langle M \rangle$, je $M \cup \{\boldsymbol{z}\} \subseteq \langle M \rangle$ a podle (2) a (3) dostáváme $\langle M \cup \{\boldsymbol{z}\} \rangle \subseteq \langle \langle M \rangle \rangle = \langle M \rangle$. Máme tedy $\langle M \rangle \subseteq \langle M \cup \{\boldsymbol{z}\} \rangle \subseteq \langle M \rangle$, takže v místě inkluzí musí být rovnost.

2.38. Poznámka. Vlastnost (1) věty ?? lidově řečeno znamená, že „lineární obalení“ množiny může přidat do této množiny další prvky, ale pokud tento proces zopakujeme, další prvky už podle vlastnosti (3) nezískáme.

Takové množiny, které při „lineárním obalení“ již nepřidávají žádné další prvky, jsou vždy lineárními podprostory. To ukazuje následující věta.

2.39. Věta.* Nechť L je lineární prostor, $M \subseteq L$. Množina M je lineárním podprostorem lineárního prostoru L právě tehdy, když $\langle M \rangle = M$.

Důkaz. Dokážeme nejprve „je-li M lineární podprostor, pak $\langle M \rangle = M$“. Vezmeme $\boldsymbol{z} \in \langle M \rangle$ a dokážeme, že $\boldsymbol{z} \in M$. Protože $\boldsymbol{z} \in \langle M \rangle$, existuje konečně mnoho vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \in M$ takových, že lze psát $\boldsymbol{z} = \alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_n \boldsymbol{x}_n$. Každý sčítanec leží podle vlastnosti (2) definice ?? v množině M. Podle vlastnosti (1) definice ?? v množině M leží i součet těchto vektorů, tedy $\boldsymbol{z} \in M$.

Zbývá dokázat „je-li $\langle M\rangle = M$, pak M je lineární podprostor“. Uvažujme $\boldsymbol{x} \in M$, $\boldsymbol{y} \in M$. Abychom dokázali, že M je lineární podprostor, stačí ověřit, že lineární kombinace $1\cdot\boldsymbol{x}+1\cdot\boldsymbol{y}$ leží v M a dále $\alpha\cdot\boldsymbol{x}+0\cdot\boldsymbol{y}$ leží v M. Protože $\boldsymbol{x} \in M$, $\boldsymbol{y} \in M$, je podle definice lineárního obalu každá jejich lineární kombinace prvkem $\langle M\rangle$ a podle předpokladu je $\langle M\rangle = M$. V množině M tedy leží i uvedené dvě lineární kombinace vektorů $\boldsymbol{x}, \boldsymbol{y}$.

2.40. Věta.* Nechť L je lineární prostor a $M \subseteq L$ je libovolná neprázdná množina. Pak $P = \langle M\rangle$ je nejmenší lineární podprostor, pro který platí $M \subseteq P$.

Důkaz. Protože $\langle P\rangle = \langle\langle M\rangle\rangle = \langle M\rangle = P$, je podle věty ?? zřejmé, že P je lineární podprostor. Stačí ukázat, že P je nejmenší podprostor s vlastností $M \subseteq P$.

Nechť Q je nějaký podprostor, pro který také platí $M \subseteq Q$. Podle věty ?? je $\langle Q\rangle = Q$. Dále použijeme (2) věty ?? na inkluzi $M \subseteq Q$ a dostáváme $P = \langle M\rangle \subseteq \langle Q\rangle = Q$.

2.41. Definice. Nechť P je lineární podprostor lineárního prostoru L. Množina vektorů M, pro kterou platí $\langle M\rangle = P$, se nazývá *množina generátorů* lineárního podprostoru P. Je-li $\langle \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\rangle = P$, pak také říkáme, že *vektory* $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ *generují* lineární podprostor P. Skutečnost, že vektory generují lineární podprostor P není nic jiného, než že množina všech jejich lineárních kombinací „vyplní“ celý podprostor P.

2.42. Věta.* Nechť L je lineární prostor, $M \subseteq L$ je lineárně nezávislá množina a $\boldsymbol{z} \notin \langle M \rangle$. Pak též $M \cup \{\boldsymbol{z}\}$ je lineárně nezávislá množina.

Důkaz. Důkaz povedeme sporem. Předpokládejme, že $M \cup \{\boldsymbol{z}\}$ je lineárně závislá. Pak existuje konečně mnoho prvků $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \in M$ takových, že $\alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_n \boldsymbol{x}_n + \alpha_{n+1} \boldsymbol{z}$ je netriviální lineární kombinace rovna nulovému vektoru. Pro $\alpha_{n+1} = 0$ zůstává netriviální lineární kombinace vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ rovna nulovému vektoru, neboli konečná podmnožina M je lineárně závislá. To je ve sporu s tím, že M je lineárně nezávislá.

Pro $\alpha_{n+1} \neq 0$ je vektor $\boldsymbol{z}$ lineární kombinací vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ (převedeme násobek vektoru $\boldsymbol{z}$ na druhou stranu rovnosti a podělíme $-\alpha_{n+1}$, jako v důkazu věty ??). To je ve sporu s tím, že $\boldsymbol{z} \notin \langle M \rangle$. Pro oba případy hodnot α_{n+1} dostáváme spor, takže $M \cup \{\boldsymbol{z}\}$ nemůže být lineárně závislá.

2.43. Věta. Nechť M a N jsou lineárně nezávislé množiny v lineárním prostoru L a předpokládejme, že $\langle M \rangle \cap \langle N \rangle = \{\boldsymbol{o}\}$. Pak množina $M \cup N$ je lineárně nezávislá.

Důkaz. Lineární nezávislost množiny $M \cup N$ vyplyne z toho, že každá konečná lineární kombinace vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m$ z M a vektorů $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_n$ z N (dohromady), která je rovna nulovému vektoru, je triviální. Položme tedy

$$(\alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_m \boldsymbol{x}_m) + (\beta_1 \boldsymbol{y}_1 + \beta_2 \boldsymbol{y}_2 + \cdots + \beta_m \boldsymbol{y}_m) = \boldsymbol{o}$$

a označme první závorku $\boldsymbol{a}$ a druhou $\boldsymbol{b}$. Zřejmě je $\boldsymbol{a} \in \langle M \rangle$ a $\boldsymbol{b} \in \langle N \rangle$. Protože je $\boldsymbol{a} = -\boldsymbol{b}$ (jinak by součet nemohl být roven nulovému vektoru), je také $\boldsymbol{a} \in \langle N \rangle$. Takže $\boldsymbol{a} \in \langle M \rangle \cap \langle N \rangle$ a podle předpokladu je $\boldsymbol{a} = \boldsymbol{o}$. Protože je M lineárně nezávislá, musí být lineární kombinace v první závorce pouze triviální. Je totiž rovna nulovému vektoru $\boldsymbol{a}$. Protože je N lienárně nezávislá, musí být lineární kombinace v druhé závorce pouze triviální. Je totiž rovna nulovému vektoru $-\boldsymbol{a}$. Takže zkoumaná lineární kombinace všech vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_n$ je triviální.

2.44. Poznámka. Předpoklad $\langle M \rangle \cap \langle N \rangle = \{\boldsymbol{o}\}$ ve větě ?? je nutný. Příklad $M = \{(1,0,0), (0,1,$ $N = \{(1,0,1), (0,1,1)\}$ ilustruje situaci, kdy obě množiny jsou lineárně nezávislé, množina M leží mimo $\langle N \rangle$ a množina N leží mimo $\langle M \rangle$, a přesto je množina $M \cup N$ lineárně závislá.

2.45. Věta. Nechť N je lineárně nezávislá množina v linerním prostoru L a nechť N_1 a N_2 jsou její disjunktní podmnožiny (tj. $N_1 \cap N_2 = \emptyset$). Pak $\langle N_1 \rangle \cap \langle N_2 \rangle = \{\boldsymbol{o}\}$.

Důkaz (pro hloubavé čtenáře). Předpokládejme $\boldsymbol{x} \in \langle N_1 \rangle \cap \langle N_2 \rangle$. Ukážeme, že musí $\boldsymbol{x} = \boldsymbol{o}$. Vektor $\boldsymbol{x}$ je konečnou lineární kombinací vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m$ z N_1 a je také konečnou lineární kombinací vektorů $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_k$ z N_2, tedy

$$\boldsymbol{x} = \alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_m \boldsymbol{x}_m, \quad \boldsymbol{x} = \beta_1 \boldsymbol{y}_1 + \beta_2 \boldsymbol{y}_2 + \cdots + \beta_k \boldsymbol{y}_k,$$

takže: $\boldsymbol{x} - \boldsymbol{x} = \boldsymbol{o} = \alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_m \boldsymbol{x}_m - \beta_1 \boldsymbol{y}_1 - \beta_2 \boldsymbol{y}_2 - \cdots - \beta_k \boldsymbol{y}_k$

Lineární kombinace $\alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_m \boldsymbol{x}_m - \beta_1 \boldsymbol{y}_1 - \beta_2 \boldsymbol{y}_2 - \cdots - \beta_k \boldsymbol{y}_k$ je kombinací konečně mnoha různých vektorů z množiny N a tato množina je podle předpokladu linárně nezávislá. Protože je tato lineární kombinace rovna nulovému vektoru, musí být triviální. Takže také $\alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_m \boldsymbol{x}_m$ je triviální lineární kombinace a to znamená, že $\boldsymbol{x} = 0\,\boldsymbol{x}_1 + 0\,\boldsymbol{x}_2 + \cdots + 0\,\boldsymbol{x}_m = \boldsymbol{o}$.

2.46. Věta. Nechť L je lineární prostor. Množina $N \subseteq L$ je lineárně nezávislá právě tehdy, když pro všechny vlastní podmnožiny $M \subset N$, $M \neq N$ platí $\langle M \rangle \subset \langle N \rangle$, $\langle M \rangle \neq \langle N \rangle$.

Důkaz (pro hloubavé čtenáře). Předpokládejme nejprve, že N je lineárně nezávislá. Nechť $M \subset N$, $M \neq N$. Zvolme vektor $\boldsymbol{z} \in N$ takový, že $\boldsymbol{z} \notin M$. Vektor $\boldsymbol{z}$ nelze vyjádřit jako lineární kombinaci žádné konečné podmnožiny prvků množiny M. Kdyby to bylo možné, byla by množina N lineárně závislá a ona není. Platí tedy, že $\boldsymbol{z} \notin \langle M \rangle$, a přitom $\boldsymbol{z} \in \langle N \rangle$.

Předpokládejme nyní, že N je lineárně závislá. Pak podle poznámky ?? existuje vektor $\boldsymbol{z} \in N$, který je roven lineární kombinaci konečně mnoha ostatních vektorů z N, takže $\boldsymbol{z} \in \langle M \rangle$, kde $M = N \setminus \{\boldsymbol{z}\}$. Podle vlastnosti (4) věty ?? je $\langle M \rangle = \langle M \cup \{\boldsymbol{z}\} \rangle$, jinými slovy $\langle M \rangle = \langle N \rangle$.

2.47. Shrnutí. V této kapitole jsme definovali lineární závislost a nezávislost vektorů /??, ??, ??, ??/. Vektory jsou lineárně závislé, pokud exituje netriviální lineární kombinace těchto vektorů rovnající se nulovému vektoru. To je ekvivalentní s tím, že existuje jeden vektor,

který je lineární kombinací ostatních /??/. Vektory jsou lineárně nezávislé, pokud jen jejich triviální lineární kombinace je rovna nulovému vektoru. Tedy pokud neexistuje žádný takový vektor, který by byl lineární kombinací ostatních.

Nekonečná množina vektorů je lineárně závislá, pokud existuje její konečná lineárně závislá podmnožina. Nekonečná množina je lineárně nezávislá, pokud každá její konečná množina je lineárně nezávislá. Každá podmnožina (konečná i nekonečná) lineárně nezávislé množiny je lineárně nezávislá /??/.

Lineární obaly vektorů obsahují všechny jejich konečné lineární kombinace /??, ??, ??/. Lineární obal lineárního obalu už nepřináší nové lineární kombinace /??/. Každý lineární podprostor P lze zapsat jako lineární obal nějaké množiny (například množiny P samotné, ale to není nejúčelnější) a naopak lineární obal jakékoli množiny M je podprostorem. Je to nejmenší podprostor, který obsahuje množinu M /??/.

Z lineárně závislé množiny lze odebrat vektor tak, aby zůstal zachován její lineární obal /??, ??/, zatímco z lineárně nezávislé množiny nelze odebrat vektor bez změny jejího lineárního obalu /??/.

3. Báze, dimenze, souřadnice

3.1. Poznámka. Mezi množinami generátorů nějakého lineárního (pod)prostoru bude zřejmě nejúspornější taková množina, která je lineárně nezávislá. Věta ?? nám ukázala, že to je skutečně „nejúspornější opatření“, protože odebráním jakéhokoli prvku z takové množiny způsobí, že lineární obal už nebude pokrývat celý (pod)prostor. Žádné prvky lineárně nezávislé množiny tedy nejsou při popisu (pod)prostoru pomocí lineárního obalu zbytečné. To nás vede (kromě jiných důležitých důvodů) k definici báze lineárního (pod)prostoru.

3.2. Definice.* *Báze* lineárního (pod)prostoru L je taková podmnožina $B \subseteq L$, pro kterou platí

(1) B je lineárně nezávislá,
(2) $\langle B \rangle = L$.

Stručně řečeno: báze lineárního (pod)prostoru L je lineárně nezávislá množina jeho generátorů.

3.3. Příklad. Množina vektorů $B = \{(1,2,3),(1,0,2),(-2,1,0)\}$ je bází lineárního prostoru $\mathbf{R}^3$, protože je podle příkladu ?? lineárně nezávislá a podle příkladu ?? generuje $\mathbf{R}^3$.

3.4. Příklad. Množina vektorů $B = \{(1,0,0),(0,1,0),(0,0,1)\}$ je bází lineárního prostoru $\mathbf{R}^3$. Snadno zjistíme, že je lineárně nezávislá a navíc pro vektor $(a,b,c) \in \mathbf{R}^3$ je

$$(a,b,c) = a\,(1,0,0) + b\,(0,1,0) + c\,(0,0,1).$$

Každý vektor (a,b,c) lze tedy zapsat jako lineární kombinaci vektorů z B, neboli $\langle B\rangle = \mathbf{R}^3$.

Všimněme si, že jsme už našli dvě báze lineárního prostoru $\mathbf{R}^3$ (v příkladu ?? a v tomto příkladu). Vidíme tedy, že báze není určena lineárním prostorem jednoznačně. Například pro $\alpha \neq 0$ jsou množiny $B_\alpha = \{(\alpha,0,0),(0,1,0),(0,0,1)\}$ různé báze lineárního prostoru $\mathbf{R}^3$. Bází je tedy nekonečně mnoho.

3.5. Příklad. Množina uspořádaných n-tic $S_n = \{(1,0,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,0,0,\ldots,$ tvoří bázi lineárního prostoru $\mathbf{R}^n$. Je lineárně nezávislá a generuje $\mathbf{R}^n$ z analogických důvodů, jako v příkladu ??. Takovou bázi lineárního prostoru $\mathbf{R}^n$ nazýváme *standardní bází*.

3.6. Příklad. Množina $B = \{1, x, x^2, x^3, \ldots\}$ tvoří bázi lineárního prostoru P všech polynomů. Podle příkladu ?? je lineárně nezávislá. Zbývá tedy ověřit, že $\langle B\rangle = P$. Zvolme nějaký polynom $p \in P$. Ukážeme, že $p \in \langle B\rangle$. Pro každý polynom $p \in P$ existuje $n \in \mathbf{N}$ a reálná čísla $a_0, a_1, \ldots, a_n$ taková, že hodnota polynomu p v bodě x je dána vzorcem

$$p(x) = a_n\,x^n + \cdots + a_1\,x + a_0 \quad \forall x \in \mathbf{R}.$$

Existuje tedy konečná podmnožina $K \subseteq B$, $K = \{1, x, x^2, \ldots, x^n\}$ taková, že p je lineární kombinací prvků z K (koeficienty této lineární kombinace jsou čísla $a_0, a_1, \ldots, a_n$). Z toho plyne, že $p \in \langle B \rangle$.

3.7. Příklad. Uvažujme lineární prostor $P_{\leq n}$ všech polynomů nejvýše n-tého stupně z příkladu ??. Ukážeme, že množina $B_n = \{1, x, x^2, \ldots, x^n\}$ tvoří bázi lineárního prostoru $P_{\leq n}$.

Předně, B_n je lineárně nezávislá, protože je podmnožinou lineárně nezávislé množiny B z příkladu ?? (každá podmnožina lineárně nezávislé množiny je podle věty ?? lineárně nezávislá). Analogicky jako v příkladu ?? lze ukázat, že $\langle B_n \rangle = P_{\leq n}$.

3.8. Příklad. Vraťme se k lineárnímu prostoru U_O všech orientovaných úseček se společným počátkem. Podle (5) z příkladu ?? je každá lineárně nezávislá množina vektorů $\{\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}\}$ bází lineárního prostoru U_O.

3.9. Poznámka.* *O existenci a jednoznačnosti báze.* Příklad ?? ilustroval skutečnost, že báze lineárního (pod)prostoru není určena jednoznačně. Lineární (pod)prostor může mít dokonce nekonečně mnoho bází.

Následující věta dokládá, že každý lineární prostor má bázi. Výjimkou je pouze triviální lineární prostor $L = \{\boldsymbol{o}\}$, který jediný nemá bázi (někteří autoři uvádějí prázdnou množinu jako bázi triviálního lineárního prostoru). Následující věta dokonce tvrdí, že každou lineárně nezávislou množinu lze doplnit přidáním případně dalších prvků na bázi a naopak, z každé

množiny M, která generuje L, lze případně odebrat nějaké prvky tak, aby zbylá množina tvořila bázi.

3.10. Věta. Nechť L je netriviální lineární prostor. Pak L má bázi. Podrobněji:
(1) Pro každou lineárně nezávislou množinu $N \subseteq L$ existuje báze B prostoru L taková, že $N \subseteq B$.
(2) Pro každou množinu M generátorů prostoru L existuje báze B prostoru L taková, že $B \subseteq M$.

Důkaz (pro hloubavé čtenáře). Tímto důkazem se čtenář opravdu nemusí zabývat, pokud k tomu nemá pádný důvod. Je zde uveden zejména proto, aby každá zde vyslovená a použitá věta měla svůj důkaz. Ovšem pro argumenty důkazu je třeba sáhnout do jiné teorie, v tomto případě axiomatické teorie množin (axiom výběru, princip maximality). Nemá-li čtenář z této oblasti odpovídající znalosti, udělá dobře, když důkaz přeskočí. Algebraická idea důkazu ve srozumitelné podobě je vyložena v následujících příkladech ??, ??, ??. To je pro studium lineární algebry dostačující. Následující důkaz je tedy spíše cvičením z teorie množin.

Důkaz existence báze se opírá o princip maximality, o kterém je známo, že je ekvivalentní s axiomem výběru. Tento axiom v teorii množin je sice bezesporný s ostatními axiomy, ale diskutabilní. Nicméně v mnoha teoriích ho potřebujeme. Třeba právě nyní.

Princip maximality říká, že máme-li množinu $\mathcal{S}$ uspořádanou relací $\leq_S$ a platí-li, že každá podmnožina $\mathcal{R}$ množiny $\mathcal{S}$, ve které jsou si v relaci všechny prvky vzájemně, má horní mez

$U \in \mathcal{S}$ (tj. $\forall R \in \mathcal{R}$ je $R \leq_S U$), pak pro každý prvek $N \in \mathcal{S}$ existuje maximální prvek $B \in \mathcal{S}$ tak, že $N \leq_S B$. Maximální prvek $B \in \mathcal{S}$ ja takový, že v $\mathcal{S}$ neexistuje prvek větší, tj. neexistuje prvek $B' \in \mathcal{S}$, $B' \neq B$ tak, že $B \leq_S B'$.

Pro důkaz první části věty nechť $\mathcal{S}$ je systém všech lineárně nezávislých množin lineárního prostoru L uspořádaný relací „být podmnožinou“, tj. relací $\subseteq$. Pro každý podsystém $\mathcal{R}$, kde lze relací $\subseteq$ porovnat každou množinu s každou (jedná se tedy o systém vzájemně do sebe vnořených množin R_I) sestrojíme $U = \cup R_I$. To je horní mez, protože $R_J \subseteq \cup R_I$ pro libovolnou množinu $R_J \in \mathcal{R}$ a navíc $U \in \mathcal{S}$, neboť je lineárně nezávislá. Proč je nezávislá? Pro spor předpokládejme, že U je lineárně závislá. Pak existuje konečná lineárně závislá množina $K = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k\} \subseteq U$. Každý jednotlivý vektor $\boldsymbol{x}_i$ leží v nějaké množině $R_i \in \mathcal{R}$. Tento konečný počet množin z $\mathcal{R}$ uspořádáme podle velikosti: $R_1 \subseteq R_2 \subseteq \cdots \subseteq R_k$, takže $K \subseteq R_k$. O množině R_k se ale ví, že je lineárně nezávislá, takže nemůže obsahovat lineárně závislou podmnožinu K. To je spor, takže U je lineárně nezávislá, tedy $U \in \mathcal{S}$. Nyní pro každou lineárně nezávislou množinu N sestrojíme podle principu maximality maximální prvek $B \in \mathcal{S}$. Množina B je báze, protože je lineárně nezávislá a přidáním libovolného prvku k B už získáme množinu mimo $\mathcal{S}$, tedy množinu lineárně závislou. Takže podle věty ?? musí $\langle B \rangle = L$.

K důkazu druhé čáti věty zvolíme $\mathcal{S}$ systém všech lineárně nezávislých podmnožin množiny M uspořádaných relací $\subseteq$. Z principu maximality (podmínky se ověří stejně jako před chvílí) existuje ke množině $N = \emptyset$ maximální množina $B \in \mathcal{S}$ taková, že $\emptyset \subseteq B$. Platí $M \subseteq \langle B \rangle$. Kdyby totiž $\boldsymbol{x} \in M$ a současně $\boldsymbol{x} \notin \langle B \rangle$, pak $B \cup \{\boldsymbol{x}\}$ by byla podle věty ?? lineárně nezávislá

podmnožina M. To ale není možné, protože B je maximální. Na nerovnost $M \subseteq \langle B\rangle$ nyní uplatníme větu ??: $\langle M\rangle \subseteq \langle\langle B\rangle\rangle = \langle B\rangle$. Protože $\langle M\rangle = L$, je $\langle B\rangle = L$..

3.11. Příklad. Je-li $N = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k\}$ lineárně nezávislá množina lineárního prostoru $\mathbf{R}^n$, pak podle předchozí věty existuje množina $B = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m\}$, $m \geq k$ taková, že B je báze. Ukážeme v tomto příkladě, jak bychom takovou bázi nalezli.

Pokud už $\langle N\rangle = \mathbf{R}^n$, pak N samotná je báze a položíme $B = N$. Pokud ale $\langle N\rangle \neq \mathbf{R}^n$, pak existuje prvek $\boldsymbol{x} \in \mathbf{R}^n$, pro který $\boldsymbol{x} \notin \langle N\rangle$ Ptáme se, zda už $N \cup \{\boldsymbol{x}\}$ je báze. Podle věty ?? tato množina zůstává lineárně nezávislá. Pokud $\langle N \cup \{\boldsymbol{x}\}\rangle = \mathbf{R}^n$, pak jsme našli bázi. Jestliže tato vlastnost neplatí, opakujme postup s přidáním dalšího prvku $\boldsymbol{y} \notin \langle N \cup \{\boldsymbol{x}\}\rangle$ znovu. Tento postup budeme opakovat tak dlouho, dokud budou existovat vektory mimo lineární obal naší postupně rozšiřované množiny. Podle příkladu ?? dospějeme k výsledku po konečně mnoha krocích, protože v $\mathbf{R}^n$ nelze vytvořit lineárně nezávislou množinu, která by měla více než n prvků.

Poznamenejme, že tento postup vedl k cíli, protože jsme měli zaručeno, že báze bude mít konečně mnoho prvků. Pro nekonečné báze bychom se tímto postupem mohli „utopit v nekonečnu“. Na druhé straně postup lze aplikovat na libovolný lineární prostor, který má konečné báze, nemusíme se nutně omezovat na $\mathbf{R}^n$.

3.12. Příklad. Tvrzení druhé části věty ?? si ilustrujeme na příkladu konečné množiny M. Je $\langle M\rangle = L$ a máme dokázat, že existuje $B \subseteq M$ taková, že $\langle B\rangle = L$ a navíc B je lineárně nezávislá.

Uvažujme všechny podmnožiny $A_i \subseteq M$, pro které $\langle A_i\rangle = L$. Vidíme, že existuje aspoň jedna taková podmnožina, sice množina M samotná. Ze všech takových podmnožin A_i vyberme tu, která má nejmenší počet prvků (všechny tyto podmnožiny jsou konečné, takže pro každou můžeme spočítat její počet prvků). Je možné, že takových množin s nejmenším počtem prvků bude existovat více, pak je jedno, kterou z nich zvolíme. Označme ji B. Víme, že $\langle B\rangle = L$ (tuto vlastnost mají všechny podmnožiny A_i, takže jmenovitě též množina B). Dále víme, že odebráním jakéhokoli prvku z množiny B už nebude pro novou B_1 platit $\langle B_1\rangle = L$. Kdyby to platilo, tak nebyla vybrána B s nejmenším počtem prvků. Nyní použijeme větu ??. Množina B je tedy lineárně nezávislá.

3.13. Příklad.* Z konečné množiny M, která splňuje $\langle M\rangle = L$, lze vytvořit postupným odebíráním prvků z M bázi L, tedy najít množinu B z předchozího příkladu. Existuje k tomu tento názorný postup: Je-li M lineárně nezávislá, je $B = M$ a jsme hotovi. Je-li lineárně závislá, podle věty ?? existuje jeden prvek M, který je lineární kombinací ostatních. Odebráním tohoto prvku vzniká množina M' se stejným lineárním obalem, jako $\langle M\rangle$, protože platí (4) věty ??. Je-li M' lineárně nezávislá, je $B = M'$ a jsme hotovi. Jinak postup opakujeme, tj. odebereme z M' vektor tak, že se nezmění lineární obal a znovu se ptáme na lineární nezávislost zbylé množiny. Proces končí, až se podaří odebrat tolik prvků, že zbytek je množina

lineárně nezávislá. Proces určitě skončí po konečně mnoha krocích, neboť M je konečná. Pokud M obsahuje nenulové vektory, výsledná množina B je jistě neprázdná, lineárně nezávislá a $\langle B\rangle = L$, tedy B je báze.

3.14. Poznámka. Příklad báze prostoru F_D všech funkcí definovaných na množině $D \subset \mathbf{R}$ nebudeme uvádět, protože nemáme prostředky, jak takovou bázi zapsat. Báze je v tomto případě nekonečnou množinou, která má větší mohutnost, než je mohutnost množiny přirozených čísel. Není tedy možné bázové prvky očíslovat a seřadit za sebe.

3.15. Poznámka. Ukážeme, že dvě (obecně různé) báze stejného lineárního (pod)prostoru mají stejný počet prvků. Tento důkaz se tradičně opírá o Steinitzovu větu o výměně. Čtenář si může pro větší názornost vytvořit množinu M černých kamínků a lineárně nezávislou množinu N bílých kamínků, které všechny leží v lineárním obalu černých. Může začít *vyměňovat* postupně černé kamínky za bílé kus za kus. Při použití následující Steinitzovy věty o výměně čtenář shledá, že výměnu lze udělat tak, aby lineární obal původní množiny M zůstal zachován i přesto, že v ní jsou nahrazeny některé černé kameny všemi bílými.

3.16. Věta (Steinitzova o výměně). Nechť L je lineární prostor, $M \subseteq L$ je libovolná množina a $N \subseteq \langle M\rangle$ je lineárně nezávislá množina, obsahující k vektorů. Pak lze odebrat z množiny M jejích k vektorů a vytvořit tak množinu M_1, pro kterou platí:

$$\langle M\rangle = \langle M_1 \cup N\rangle.$$

Jinými slovy, odebráním vhodných k vektorů z M a nahrazením těchto vektorů všemi lineárně nezávislými vektory z N se lineární obal $\langle M\rangle$ nezmění.

Důkaz (pro hloubavé čtenáře). Použijeme matematickou indukci podle k (o indukci viz důkaz věty ??). Pro $k = 0$ věta platí, protože množinu M vůbec neměníme.

Nechť nyní věta platí pro každou lineárně nezávislou množinu s k prvky a dokážeme, že platí i pro množinu s $k + 1$ prvky. Nechť $N = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k, \boldsymbol{v}_{k+1}\} \subseteq \langle M\rangle$. Označme $N_1 = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k\}$. Z množiny M lze odebrat k vektorů tak, že vznikne množina M_1, pro kterou je

$$\langle M\rangle = \langle M_1 \cup N_1\rangle = \langle M_1 \cup N\rangle.$$

První rovnost je indukční předpoklad a druhá rovnost plyne z toho, že $\boldsymbol{v}_{k+1} \in \langle M\rangle = \langle M_1 \cup N_1\rangle$ a ze čtvrté vlastnosti věty ??. Stačí tedy najít v M_1 vektor $\boldsymbol{w}_1$ tak, aby jej šlo odebrat a obal se nezměnil, tedy $\langle M_1 \cup N\rangle = \langle M_1 \setminus \{\boldsymbol{w}_1\} \cup N\rangle$. Protože $\boldsymbol{v}_{k+1} \in \langle M\rangle = \langle M_1 \cup N_1\rangle$, existuje konečně mnoho vektorů $\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_n \in M_1$ tak, že

$$\boldsymbol{v}_{k+1} = \alpha_1\boldsymbol{w}_1 + \alpha_2\boldsymbol{w}_2 + \cdots + \alpha_n\boldsymbol{w}_n + \beta_1\boldsymbol{v}_1 + \cdots + \beta_k\boldsymbol{v}_k.$$

Protože N je lineárně nezávislá, tak (A) při $k = 0$ musí být $\boldsymbol{v}_{k+1}$ nenulový a (B) při $k > 0$ nesmí $\boldsymbol{v}_{k+1}$ být lineární kombinací vektorů $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$ (věta ??). Z toho plyne, že $n > 0$ a nemohou být všechny koeficienty α_i nulové. Uspořádáme nyní $\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_n$ tak, aby $\alpha_1 \neq 0$.

Z předchozí rovnosti plyne

$$\boldsymbol{w}_1 = \frac{1}{\alpha_1}\,\boldsymbol{v}_{k+1} - \frac{\alpha_2}{\alpha_1}\,\boldsymbol{w}_2 - \cdots - \frac{\alpha_n}{\alpha_1}\,\boldsymbol{w}_n - \frac{\beta_1}{\alpha_1}\,\boldsymbol{v}_1 - \cdots - \frac{\beta_k}{\alpha_1}\,\boldsymbol{v}_k,$$

takže $\boldsymbol{w}_1 \in \langle M_1 \setminus \{\boldsymbol{w}_1\} \cup N_1 \cup \{\boldsymbol{v}_{k+1}\}\rangle$. Podle (4) z věty ?? se přidáním vektoru $\boldsymbol{w}_1$ do množiny $M_1 \setminus \{\boldsymbol{w}_1\} \cup N$ lineární obal množiny nezmění, takže je $\langle M_1 \setminus \{\boldsymbol{w}_1\} \cup N\rangle = \langle M_1 \cup N\rangle = \langle M\rangle$. Uvedený postup přitom zaručil $\boldsymbol{w}_1 \in M_1$, takže z množiny M jsme celkem odebrali $k+1$ vektorů.

3.17. Věta. Nechť L je lineární prostor, $M \subseteq L$ je libovolná konečná množina a $N \subseteq \langle M\rangle$ je lineárně nezávislá množina. Pak počet prvků množiny N je menší nebo roven počtu prvků množiny M.

Důkaz. Věta ?? tvrdí, že z množiny M lze odebrat tolik vektorů, kolik jich má množina N. Kdyby měla množina N více vektorů než množina M, pak by tento úkon nešel provést, tj. dostali bychom se do sporu se Steinitzovou větou.

3.18. Věta.* Dvě báze stejného lineárního prostoru jsou obě nekonečné nebo mají stejný počet prvků.

Důkaz. Uvažujme dvě konečné báze B_1 a B_2 lineárního prostoru L. Protože $B_1 \subseteq \langle B_2\rangle$ a B_1 je lineárně nezávislá, musí podle věty ?? mít B_2 aspoň tolik prvků, jako má B_1. Protože

$B_2 \subseteq \langle B_1 \rangle$ a B_2 je lineárně nezávislá, musí podle stejné věty mít B_1 aspoň tolik prvků, jako má B_2. Takže počet prvků těchto množin musí být stejný.

Co se stane, když B_1 je konečná a B_2 nekonečná? Pak každá konečná podmnožina $K \subseteq B_2$ je lineárně nezávislá. Vezmu takovou konečnou podmnožinu K, která má více prvků, než B_1. Protože $K \subseteq \langle B_1 \rangle$ a K je lineárně nezávislá, musí mít B_1 aspoň tolik prvků, jako K. To ale nemá. Dostáváme tedy spor, takže situace „jedna báze konečná a druhá nekonečná“ nemůže nastat.

3.19. Definice.* *Dimenze* lineárního (pod)prostoru L je počet prvků báze tohoto (pod)prostoru Dimenzi (pod)prostoru L označujeme symbolem $\dim L$. Dimenzi jednobodového lineárního (pod)prostoru $L = \{\boldsymbol{o}\}$ pokládáme rovnu nule.

3.20. Poznámka. Věta ?? nám zaručuje smysluplnost definice dimenze. Ačkoli lineární prostor může mít více bází, všechny tyto báze mají podle této věty stejný počet prvků, nebo jsou nekonečné. V tomto druhém případě klademe $\dim L = \infty$.

3.21. Příklad. $\dim \mathbf{R}^n = n$, viz příklad ??. $\dim P_{\leq n} = n + 1$, viz příklad ??. $\dim P = \infty$, viz příklad ??. Konečně $\dim U_O = 3$ podle příkladu ??. Važme si toho, že nás Stvořitel obklopil lineárním prostorem dimenze 3 nejen proto, že trojka je šťastné číslo.

3.22. Věta. Nechť L je lineární prostor a $P \subseteq L$ je lineární podprostor lineárního prostoru L. Pak $\dim P \leq \dim L$.

Důkaz. Označme B_L nějakou bázi lineárního prostoru L. Báze B_P podprostoru P je lineárně nezávislá množina, pro kterou je $B_P \subseteq \langle B_L \rangle$. Podle věty ?? má B_P nejvýše tolik prvků, jako B_L.

3.23. Věta. Nechť L je lineární prostor a $P \subseteq L$ je lineární podprostor lineárního prostoru L. Nechť dále $\dim P = \dim L$ a tato dimenze je konečná. Potom $P = L$.

Důkaz. B_P je báze podprostoru P a B_L báze prostoru L jako v předchozím důkazu, tj. $B_P \subseteq \langle B_L \rangle$. Protože jsou B_P a B_L stejně početné, pak podle Steinitzovy věty lze vyměnit všechny vektory z B_L za všechny vektory z B_P beze změny lineárního obalu, takže $\langle B_P \rangle = \langle B_L \rangle$. Jinými slovy $P = L$.

3.24. Poznámka. Podmínku konečnosti dimenze v předchozí větě nelze vynechat. Steinitzova věta totiž předpokládá konečnou množinu N. Nezbytnost podmínky konečné dimenze ilustruje třeba tento příklad. Nechť L je lineární prostor všech polynomů a $P = \langle 1, x^2, x^4, \ldots \rangle$ je podprostor polynomů jen se sudými mocninami. Pak $\dim L = \dim P = \infty$, ale $P \neq L$.

3.25. Poznámka. Věta ?? má důsledky shrnuté v následujících dvou větách. Ty se nám budou hodit, až budeme lineární podprostory zapisovat jako lineární obaly množin vektorů a budeme se potýkat s tím, že tento zápis podprostoru není jednoznačný.

3.26. Věta. Nechť $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k, \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$ jsou vektory lineárního prostoru L. Rovnost lineárních obalů $\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle$ a $\langle \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m \rangle$ je ekvivalentní podmínce:

$$\dim\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle = \dim\langle \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m \rangle = \dim\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k, \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m \rangle.$$

Důkaz. Přepokládejme nejprve rovnost obalů a dokážeme podmínku. Označíme $U = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots$ a $V = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m\}$. Jestliže $\langle U \rangle = \langle V \rangle$, pak $U \subseteq \langle U \rangle = \langle V \rangle$, $V \subseteq \langle U \rangle = \langle V \rangle$, tedy $U \cup V \subseteq \langle U \rangle = \langle V \rangle$. Přechodem k lineárnímu obalu obou stran množinové nerovnosti a využitím věty ?? (3) dostáváme $\langle U \cup V \rangle \subseteq \langle \langle U \rangle \rangle = \langle U \rangle$. Protože $U \cup V \supseteq U$, platí také $\langle U \cup V \rangle \supseteq \langle U \rangle$, takže $\langle U \cup V \rangle = \langle U \rangle = \langle V \rangle$. Když se rovnají obaly, rovnají se i jejich dimenze.

Předpokládejme nyní platnost podmínky a dokážeme $\langle U \rangle = \langle V \rangle$. Protože $\langle U \rangle \subseteq \langle U \cup V \rangle$ a dimenze se rovnají, musí se podle věty ?? (volte $\langle U \rangle = P, \langle U \cup V \rangle = L$) rovnat obaly samotné, tj. $\langle U \rangle = \langle U \cup V \rangle$. To samé platí pro $\langle V \rangle$, takže $\langle U \rangle = \langle U \cup V \rangle = \langle V \rangle$.

3.27. Věta. Nechť $\boldsymbol{v}, \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ jsou vektory lineárního prostoru L. Pak $\boldsymbol{v} \in \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle$ právě tehdy, když $\dim\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle = \dim\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k, \boldsymbol{v} \rangle$.

Důkaz. Z předpokladu, že $\boldsymbol{v} \in \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle$ a z věty ?? (4) plyne, že obaly $\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle$ a $\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k, \boldsymbol{v} \rangle$ se rovnají. Proto se rovnají i jejich dimenze.

Nechť nyní se dimenze rovnají. Obal $\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle$ je podprostorem obalu $\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$, takže podle věty ?? se tyto obaly rovnají. Vlastnost $\boldsymbol{v} \in \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle$ pak plyne z následující inkluze: $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k, \boldsymbol{v}\} \subseteq \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k, \boldsymbol{v} \rangle = \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle$.

3.28. Věta. Nechť L je lineární prostor, $\dim L = n$ a $M = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m\}$. Pak platí:
(1) Je-li M lineárně nezávislá, pak $m \leq n$.
(2) Je-li $m > n$, pak M je lineárně závislá.
(3) Je-li $m = n$ a M je lineárně nezávislá, pak $\langle M \rangle = L$.
(4) Je-li $m = n$ a $\langle M \rangle = L$, pak je M lineárně nezávislá.
(5) Je-li M lineárně nezávislá a $\langle M \rangle = L$, pak $m = n$.

Důkaz. (1) Nechť B je báze L, tedy $\langle B \rangle = L$. Podle věty ?? lze nahradit m prvků z B všemi prvky z M tak, že se lineární obal nezmění. Aby to bylo možné provést, nutně musí být $m \leq n$.

(2) Toto tvrzení je ekvivalentní s tvrzením (1).

(3) Kdyby $\langle M \rangle \neq L$, pak lze přidat do množiny M vektor $\boldsymbol{x} \notin \langle M \rangle$, a přitom podle věty ?? zůstane rozšířená množina lineárně nezávislá. To ale podle (1) není možné. Musí tedy $\langle M \rangle = L$.

(4) Z množiny M lze odebrat prvky tak, aby vzniklá podmnožina $B \subseteq M$ měla stejný obal, ale byla lineárně nezávislá. B je tedy bází prostoru L. Kdyby byla M lineárně závislá, pak musí B mít méně prvků než $m = n$, což je ve sporu s větou ??. Takže musí M být lineárně nezávislá.

(5) Množina M je podle definice bází L. Podle věty ?? tedy musí mít n prvků.

3.29. Poznámka. Uvědomíme si význam této věty. Báze lineárního prostoru konečné dimenze je podle (1) nejpočetnější lineárně nezávislá množina. Dále podle (3) každá lineárně nezávislá množina, která má počet prvků rovný konečné dimenzi, je bází.

3.30. Příklad. Množina $\{(1,1,1),(0,1,1),(0,0,2)\}$ je bází lineárního prostoru $\mathbf{R}^3$, protože je lineárně nezávislá a její počet prvků je roven $\dim \mathbf{R}^3$. Stačí použít větu ??, vlastnost (3) a nemusíme pracně ověřovat z definice, že množina generuje $\mathbf{R}^3$.

3.31. Poznámka. Je-li $\dim L$ konečná, je možné zvolit a uspořádat bázi prostoru L a každý vektor $\boldsymbol{x}$ pak zapsat jako lineární kombinaci této báze. Koeficienty této lineární kombinace nazýváme *souřadnice vektoru* $\boldsymbol{x}$. Tímto způsobem můžeme vektory lineárního prostoru L podchytit pomocí reálných čísel. Přechod od abstraktního vektoru k souřadnicím (uspořádané n-tici čísel) nyní popíšeme podrobněji.

3.32. Definice. Nechť $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ je báze lineárního prostoru L. Záleží-li nám na pořadí prvků báze $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n$ (tj. požadujeme, aby $\boldsymbol{b}_1$ byl první prvek báze, $\boldsymbol{b}_2$ druhý prvek atd.), pak mluvíme o *uspořádané bázi*. Uspořádaná báze je tedy uspořádaná n-tice prvků báze, tj. $(\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$. Skutečnost, že báze B je uspořádaná, budeme vyznačovat symbolem (B).

3.33. Poznámka. Uspořádanou bázi jsme definovali jen pro lineární prostory konečné dimenze. Ačkoli tedy v dalším textu nebude tato skutečnost výslovně uvedena, všude tam, kde se mluví o uspořádaných bázích, máme na mysli lineární prostor konečné dimenze.

3.34. Definice.* Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je uspořádaná báze lineárního prostoru L a $\boldsymbol{x} \in L$ je libovolný vektor. Uspořádanou n-tici reálných čísel $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbf{R}^n$ nazýváme *souřadnicemi vektoru $\boldsymbol{x}$ vzhledem k uspořádané bázi (B)*, pokud platí

$$\boldsymbol{x} = \alpha_1 \boldsymbol{b}_1 + \alpha_2 \boldsymbol{b}_2 + \cdots + \alpha_n \boldsymbol{b}_n.$$

Skutečnost, že $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ jsou souřadnice vektoru $\boldsymbol{x}$ vzhledem k uspořádané bázi (B) budeme zapisovat takto:

$$\mathcal{C}_B(\boldsymbol{x}) = (\alpha_1, \alpha_2, \ldots, \alpha_n).$$

3.35. Věta.* Nechť (B) je uspořádaná báze lineárního prostoru L. Pak každý vektor $\boldsymbol{x} \in L$ má jednoznačně určeny své souřadnice vzhledem k uspořádané bázi (B)

Důkaz. Existence: protože $\langle B \rangle = L$, lze každý vektor $\boldsymbol{x} \in L$ zapsat jako lineární kombinaci prvků z B.

Jednoznačnost: Důkaz se opírá o lineární nezávislost množiny B. Označme $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots$ Nechť $\boldsymbol{x}$ má soužadnice $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ a současně má souřadnice $(\beta_1, \beta_2, \ldots, \beta_n)$. V obou případech se jedná o souřadnice vzhledem ke stejné bázi (B). Ukážeme, že pak je $\alpha_i = \beta_i$, $\forall i \in \{1, \ldots, n\}$. Podle definice ?? je

$$\boldsymbol{x} = \alpha_1 \, \boldsymbol{b}_1 + \alpha_2 \, \boldsymbol{b}_2 + \cdots + \alpha_n \, \boldsymbol{b}_n, \qquad \boldsymbol{x} = \beta_1 \, \boldsymbol{b}_1 + \beta_2 \, \boldsymbol{b}_2 + \cdots + \beta_n \, \boldsymbol{b}_n.$$

Odečtením těchto rovností dostáváme

$$\boldsymbol{x} - \boldsymbol{x} = \boldsymbol{o} = (\alpha_1 - \beta_1) \, \boldsymbol{b}_1 + (\alpha_2 - \beta_2) \, \boldsymbol{b}_2 + \cdots + (\alpha_n - \beta_n) \, \boldsymbol{b}_n.$$

Protože vektory báze $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n$ jsou lineárně nezávislé, pouze triviální lineární kombinace může být rovna nulovému vektoru. Všechny koeficienty uvedené lineární kombinace musejí tedy být rovny nule. Tím dostáváme $\alpha_i = \beta_i$, $\forall i \in \{1, \ldots, n\}$.

3.36. Příklad. Nechť L je lineární prostor polynomů nejvýše třetího stupně. Najdeme souřadnice polynomu $p \in L$, $p(x) = 2x^3 + x^2 - 3x$ vzhledem k uspořádané bázi $(B) = \big(x+1, x-1, (x+1)^2, (x+1)^3\big)$.

Nevěřící Tomášové by nejprve měli ověřit, zda je B skutečně bází lineárního prostoru L, tj. zda platí vlastnosti (1) a (2) z definice ??. Položili by následující lineární kombinaci rovnu nulovému polynomu:

$$\alpha\,(x+1)+\beta\,(x-1)+\gamma\,(x+1)^2+\delta\,(x+1)^3 = \delta\,x^3+(\gamma+3\delta)\,x^2+(\alpha+\beta+2\gamma+3\delta)\,x+\alpha-\beta+\gamma+\delta = 0$$

a zkoumali by, za jakých okolností lze rovnost splnit. Polynom je nulový jen tehdy, když jsou nulové všechny jeho koeficienty, což vede na homogenní soustavu čtyř rovnic o neznámých $\alpha, \beta, \gamma, \delta$. Tu by Tomášové vyřešili, zjistili by, že má pouze nulové řešení, a proto jsou dané polynomy z množiny B lineárně nezávislé. Dále by Tomášové použili vlastnost (3) věty ?? a prohlásili, že když množina B je lineárně nezávislá a obsahuje stejný počet vektorů, jako je dimenze prostoru (podle příkladu ?? je $\dim L = 4$), pak musí $\langle B \rangle = L$. Tím by zjistili, že B je báze lineárního prostoru L.

Nyní najdeme souřadnice polynomu p vzhledem k bázi (B). Podle definice ?? má pro souřadnice $(\alpha, \beta, \gamma, \delta)$ platit

$$2x^3 + x^2 - 3x = \alpha\,(x+1) + \beta\,(x-1) + \gamma\,(x+1)^2 + \delta\,(x+1)^3,$$

$$\text{po úpravě:}\quad 2x^3 + x^2 - 3x = \delta\,x^3 + (\gamma+3\delta)\,x^2 + (\alpha+\beta+2\gamma+3\delta)\,x + \alpha - \beta + \gamma + \delta.$$

Dva polynomy se rovnají, když se rovnají odpovídající jejich koeficienty. Po porovnání jednotlivých koeficientů u polynomů na levé a pravé straně rovnosti dostáváme soustavu rovnic

$$\begin{aligned} \alpha - \beta + \gamma + \delta &= 0 \\ \alpha + \beta + 2\gamma + 3\delta &= -3 \\ \gamma + 3\delta &= 1 \\ \delta &= 2 \end{aligned}$$

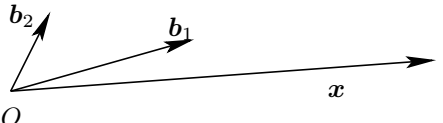
Soustava má jediné řešení $\alpha = 2, \beta = -1, \gamma = -5, \delta = 2$. Zapíšeme výsledek: $\mathcal{C}_B(p) = (2, -1, -5, 2)$.

3.37. Příklad. Uvažujme stejný lineární prostor L jako v předchozím příkladě a v něm stejný polynom $p \in L$, $p(x) = 2x^3 + x^2 - 3x$. Vzhledem k uspořádané bázi $B_0 = (1, x, x^2, x^3)$ má polynom souřadnice shodné se svými koeficienty, tedy

$$\mathcal{C}_{B_0}(p) = (0, -3, 1, 2).$$

Platí totiž $p(x) = 0 \cdot 1 + (-3) \cdot x + 1 \cdot x^2 + 2 \cdot x^3$.

3.38. Příklad. Uvažujme podprostor P prostoru orientovaných úseček U_O, ve kterém jsou jen vektory ležící v rovině dané stránkou této učebnice



a mající počáteční bod v bodě O na obrázku. Zjevně je $\dim P = 2$. Na uvedeném obrázku jsou vyznačeny vektory $\boldsymbol{b}_1$ a $\boldsymbol{b}_2 \in P$, které jsou lineárně nezávislé, takže tvoří bázi podprostoru P. Najdeme souřadnice vektoru $\boldsymbol{x}$ vzhledem k uspořádané bázi $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2)$.

Je třeba narýsovat dvě měřítka, jedno procházející vektorem $\boldsymbol{b}_1$ a mající jedničku v koncovém bodě tohoto vektoru. Druhé měřítko prochází vektorem $\boldsymbol{b}_2$ a má jedničku v koncovém bodě $\boldsymbol{b}_2$. Obě měřítka mají nulu v bodě O. Dále narýsujeme rovnoběžky s těmito měřítky, které procházejí koncovým bodem vektoru $\boldsymbol{x}$. V průsečících těchto přímek pak přečteme souřadnice vektoru $\boldsymbol{x}$. Laskavý čtenář si jistě sám do obrázku dorýsuje uvedená měřítka a rovnoběžky a shledá, že je $\mathcal{C}_B(\boldsymbol{x}) = (2{,}6;\ -1{,}3)$. Přesnost výsledku závisí na přesnosti rýsování.

Pamatujme: ideální geometrii nikdy nenarýsujeme, ta existuje pouze v myslích každého z nás. Takže ve skutečnosti jsou vektory z lineárního prostoru U_O velmi obtížně uchopitelné. Je tedy užitečné přejít od těchto abstraktních vektorů k uspořádaným n-ticím reálných čísel, k jejich souřadnicím. S těmi se počítá daleko pohodlněji. Viz též příklad ??

3.39. Příklad. V lineárním prostoru $\mathbf{R}^n$ se pracuje přímo s reálnými čísly, takže hledat k uspořádaným n-ticím jejich souřadnice, tedy zase uspořádané n-tice, může působit jako nošení dříví do lesa. Nicméně se o to pokusíme. Abychom se do toho nezamotali, rozlišujme důsledně pojem *složky vektoru* od pojmu *souřadnice vektoru* vzhledem ke zvolené bázi. Zvolíme

dvě uspořádané báze v $\mathbf{R}^3$:

$$(B) = \big((1,3,1),(3,0,2),(2,1,1)\big), \qquad (S_3) = \big((1,0,0),(0,1,0),(0,0,1)\big).$$

je dán vektor $(1,2,3)$. Čísla 1, 2, 3 jsou jeho složky a báze na předchozím řádku jsou také dány svými složkami. Najdeme souřadnice daného vektoru jednak vzhledem k bázi (B) a také vzhledem k bázi (S_3).

Především je zřejmé, že B je báze (nevěřící Tomášové si to ověří). Množina S_3 je také bází, je to dokonce standardní báze lineárního prostoru $\mathbf{R}^3$.

Souřadnice vektoru $(1,2,3)$ vzhledem k (B) tvoří trojici čísel (α,β,γ), pro které platí

$$(1,2,3) = \alpha(1,3,1) + \beta(3,0,2) + \gamma(2,1,1)$$

Po vynásobení vektorů a jejich sečtení podle definice z příkladu ?? dostáváme rovnost uspořádaných trojic $(1,2,3) = (\alpha+3\beta+2\gamma, 3\alpha+\gamma, \alpha+2\beta+\gamma)$. Z této rovnosti plynou tři rovnice pro neznámé α,β,γ. Čtenář si sám spočítá, že soustava těchto tří rovnic má jediné řešení $\alpha = 9/4$, $\beta = 11/4$, $\gamma = -19/4$. Takže $\mathcal{C}_B\big((1,2,3)\big) = (9/4, 11/4, -19/4)$.

Protože je $(1,2,3) = 1\cdot(1,0,0) + 2\cdot(0,1,0) + 3\cdot(0,0,1)$, je okamžitě patrné, že $\mathcal{C}_{S_3}\big((1,2,3)\big) = (1,2,3)$. Poslední výsledek zobecníme v následujícím tvrzení:

3.40. Věta. Souřadnice každého vektoru $\boldsymbol{x} \in \mathbf{R}^n$ vzhledem ke standardní bázi S_n jsou rovny složkám vektoru $\boldsymbol{x}$. Jinými slovy: $\mathcal{C}_{S_n}\big((x_1,x_2,\ldots,x_n)\big) = (x_1,x_2,\ldots,x_n)$.

Důkaz. Zřejmě je $(x_1,x_2,\ldots,x_n) = x_1(1,0,0,\ldots,0)+x_2(0,1,0,\ldots,0)+\ldots+x_n(0,0,0,\ldots,0,1)$.

3.41. Poznámka.* Výše uvedené příklady ilustrují platnost sloganu „na volbě báze záleží“. Především vidíme, že souřadnice stejného vektoru vzhledem k různým bázím jsou rozdílné.

V příkladě ?? se nám podařilo najít souřadnice stejného polynomu mnohem pohodlněji, než v příkladě ??. Stejně tak by se nám lépe hledaly souřadnice orientované úsečky v příkladě ??, pokud by byly bázové vektory voleny tak, že jsou na sebe kolmé a mají stejnou velikost. Mohli bychom pak použít pravítko s ryskou. Konečně standardní báze (B_0) v $\mathbf{R}^3$ v příkladu ?? nám nekladla (na rozdíl od náhodně zvolené báze B) žádné překážky při hledání souřadnic. Mezi všemi bázemi lineárního prostoru tedy existují báze, vzhledem ke kterým je možné hledat souřadnice výrazně pohodlněji.

3.42. Definice. Nechť L je lineární prostor, M a N jsou jeho podprostory. Množinu $\langle M \cup N \rangle$ nazýváme *spojením podprostorů M a N* a značíme $M \vee N$.

3.43. Poznámka. Podle věty ?? je $M \vee N$ nejmenší podprostor, který obsahuje všechny prvky z M i N dohromady.

3.44. Věta. Nechť L je lineární prostor, M a N jsou jeho podprostory. Pro podprostor $M \vee N$ platí:

$$M \vee N = \{\boldsymbol{y} + \boldsymbol{z};\ \boldsymbol{y} \in M,\ \boldsymbol{z} \in N\}.$$

Důkaz. Je-li $\boldsymbol{x} \in \{\boldsymbol{y}+\boldsymbol{z};\ \boldsymbol{y} \in M, \boldsymbol{z} \in N\}$, tj. $\boldsymbol{x}$ se dá rozepsat na součet prvku z M a prvku z N, pak podle definice lineárního obalu je $\boldsymbol{x} \in \langle M \cup N\rangle = M \vee N$. To dokazuje inkluzi $\{\boldsymbol{y}+\boldsymbol{z};\ \boldsymbol{y} \in M, \boldsymbol{z} \in N\} \subseteq M \vee N$.

Je-li $\boldsymbol{x} \in M \vee N = \langle M \cup N\rangle$, pak podle definice lineárního obalu existuje konečně mnoho prvků z M a konečně mnoho prvků z N takových, že $\boldsymbol{x}$ je lineární kombinací těchto prvků. Tuto lineární kombinaci rozdělíme na součet násobků prvků z M a součet násobků ostatních prvků (tedy prvků z N). První součet označíme $\boldsymbol{y}$ a druhý $\boldsymbol{z}$. Protože M a N jsou podprostory, je podle věty ?? $\langle M\rangle = M$, $\langle N\rangle = N$, takže lineární kombinace prvků z M leží v M a podobně pro N. Máme tedy $\boldsymbol{y} \in M$, $\boldsymbol{z} \in N$. Protože $\boldsymbol{x} = \boldsymbol{y}+\boldsymbol{z}$, je $\boldsymbol{x} \in \{\boldsymbol{y}+\boldsymbol{z};\ \boldsymbol{y} \in M, \boldsymbol{z} \in N\}$. To dokazuje obrácenou inkluzi.

3.45. Věta.* Nechť L je lineární prostor konečné dimenze, M a N jsou jeho podprostory. Pak

$$\dim M + \dim N = \dim(M \cap N) + \dim(M \vee N).$$

Důkaz (pro hloubavé čtenáře). Nechť $\dim M = m$, $\dim N = n$, $\dim(M \cap N) = k$. Nechť $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$ je báze podprostoru $M \cap N$. Vzhledem k tomu, že $M \cap N \subseteq M$, lze lineárně nezávislé vektory $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$ doplnit o další prvky, aby dohromady tvořily bázi v M. Viz větu ??. Podobně lze doplnit $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$ o další prvky, aby tvořily bázi v N. Máme tedy

$$\text{báze } M \cap N: \qquad \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k\},$$

$$\begin{array}{ll} \text{báze } M\text{:} & \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k, \boldsymbol{c}_{k+1}, \ldots, \boldsymbol{c}_m\}, \\ \text{báze } N\text{:} & \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k, \boldsymbol{d}_{k+1}, \ldots, \boldsymbol{d}_n\}. \end{array}$$

Za této situace je množina $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k, \boldsymbol{c}_{k+1}, \ldots, \boldsymbol{c}_m, \boldsymbol{d}_{k+1}, \ldots, \boldsymbol{d}_n\}$ bází podprostoru $M \vee N$. Zdůvodníme proč.

Ukážeme nejdříve, že $\langle B \rangle = M \vee N$. Protože $B \subseteq M \cup N$, je $\langle B \rangle \subseteq \langle M \cup N \rangle = M \vee N$. Nyní ukážeme obrácenou inkluzi. Je-li $\boldsymbol{x} \in M \vee N$, pak podle věty ?? existují vektory $\boldsymbol{y} \in M$ a $\boldsymbol{z} \in N$ takové, že $\boldsymbol{x} = \boldsymbol{y} + \boldsymbol{z}$. Vektor $\boldsymbol{y}$ lze zapsat jako lineární kombinaci prvků báze M a vektor $\boldsymbol{z}$ jako lineární kombinaci prvků báze N. Proto je vektor $\boldsymbol{x}$ lineární kombinací prvků množiny B a máme dokázánu obrácenou inkluzi $M \vee N \subseteq \langle B \rangle$.

Nyní ukážeme, že B je lineárně nezávislá množina. Položme

$$(\alpha_1 \boldsymbol{b}_1 + \alpha_2 \boldsymbol{b}_2 + \cdots + \alpha_k \boldsymbol{b}_k) + (\gamma_{k+1}\boldsymbol{c}_{k+1} + \cdots + \gamma_m \boldsymbol{c}_m) + (\delta_{k+1}\boldsymbol{d}_{k+1} + \cdots + \delta_m \boldsymbol{d}_m) = \boldsymbol{o}.$$

Dokážeme, že tato lineární kombinace musí být triviální. Označme první závorku $\boldsymbol{b}$, druhou $\boldsymbol{c}$ a třetí $\boldsymbol{d}$. Je $\boldsymbol{d} = -\boldsymbol{b} - \boldsymbol{c}$, takže $\boldsymbol{d} \in M$ (je lineární kombinací prvků z M) a také $\boldsymbol{d} \in N$ (je lineární kombinací prvků s N), takže $\boldsymbol{d} \in M \cap N$. Je tedy možné zapsat $\boldsymbol{d}$ jako lineární kombinaci prvků báze $M \cap N$, tedy $\boldsymbol{d} = \beta_1 \boldsymbol{b}_1 + \beta_2 \boldsymbol{b}_2 + \cdots + \beta_k \boldsymbol{b}_k$. Jinak napsáno: $\beta_1 \boldsymbol{b}_1 + \beta_2 \boldsymbol{b}_2 + \cdots + \beta_k \boldsymbol{b}_k - \delta_{k+1}\boldsymbol{d}_{k+1} - \cdots - \delta_m \boldsymbol{d}_m = \boldsymbol{o}$. Tady vidíme lineární kombinaci prvků báze podprostoru N rovnu nulovému vektoru, takže musí být triviální. Takže $\boldsymbol{d} = \boldsymbol{o}$. Dosadíme tento poznatek do původní rovnosti $\boldsymbol{b}+\boldsymbol{c}+\boldsymbol{d} = \boldsymbol{o}$ a máme $\boldsymbol{b}+\boldsymbol{c} = \boldsymbol{o}$, jinak napsáno:

$\alpha_1 \boldsymbol{b}_1 + \alpha_2 \boldsymbol{b}_2 + \cdots + \alpha_k \boldsymbol{b}_k + \gamma_{k+1}\boldsymbol{c}_{k+1} + \cdots + \gamma_m \boldsymbol{c}_m = \boldsymbol{o}$. Zde je lineární kombinace prvků báze podprostoru M, která je rovna nulovému vektoru. Takže musí být triviální.

Protože B je bází $M \vee N$ a je vidět, že B má $m+n-k$ prvků, je $\dim(M \vee N) = m+n-k$. Dokazovaná rovnost nyní plyne z toho, že platí $m + n = k + (m + n - k)$.

3.46. Shrnutí. Lineárně nezávislou množinu vektorů, která generuje lineární (pod)prostor, nazýváme bází tohoto (pod)prostoru /??/. Bází stejného (pod)prostoru je více, ale všechny mají stejný počet prvků /??, ??/. Tento počet prvků se nazývá dimenze (pod)prostoru /??/.

Konečná lineárně nezávislá množina je bází (pod)prostoru L, pokud má stejný počet prvků, jako je dimenze L /??/. Více prvků lineárně nezávislá množina nemůže mít /rovněž ??/, takže dimenze L je maximální počet prvků, jaký může v L mít lineárně nezávislá množina.

Každý vektor $\boldsymbol{x}$ lineárního prostoru konečné dimenze má vzhledem k pevně zvolené uspořádané bázi jednoznačně určeny své souřadnice. Stačí vektor $\boldsymbol{x}$ zapsat jako lineární kombinaci prvků této báze a koeficienty této kombinace nazýváme jeho souřadnice /??, ??/. Existence souřadnic je dána tím, báze generuje prostor a jednoznačnost plyne z lineární nezávislosti báze.

Vzhledem k různým bázím má stejný vektor samozřejmě různé souřadnice. Existují báze, vzhledem ke kterým se souřadnice pohodlně hledají /??, ??/, zatímco najít souřadnice vektoru vzhledem k jiným bázím dá poněkud práci /??, ??, ??/. Pomocí souřadnic můžeme numericky podchytit vektory z rozličných lineárních prostorů. Přesná formulace této velmi důležité vlastnosti bude předmětem až další kapitoly.

V závěru kapitoly jsme zavedli pojem spojení podprostorů /??/ a dokázali důležitou větu o dimenzi spojení a průniku dvou lineárních podprostorů /??/.

4. Lineární zobrazení, izomorfismus

4.1. Poznámka. Zobrazení je zobecněním pojmu funkce. Zatímco funkce přiřazuje číslům čísla, zobrazení přiřazuje prvkům libovolné množiny prvky libovolné množiny.

Než se pustíme do definice pojmu *lineární* zobrazení, bude užitečné si připomenout, co to je vůbec zobrazení, a uvést jeho základní vlastnosti.

4.2. Definice. Nechť L_1 a L_2 jsou libovolné množiny. *Zobrazením $\mathcal{A}$ z množiny L_1 do množiny L_2* rozumíme jakýkoli předpis, který každému prvku z množiny L_1 přiřadí jednoznačným způsobem nějaký prvek z množiny L_2. Skutečnost, že $\mathcal{A}$ je zobrazení z množiny L_1 do množiny L_2, zapisujeme $\mathcal{A}\colon L_1 \to L_2$.

Je-li $\boldsymbol{x} \in L_1$, pak zobrazení $\mathcal{A}\colon L_1 \to L_2$ přiřadí prvku $\boldsymbol{x}$ jednoznačně nějaký prvek z množiny L_2. Tento prvek označujeme symbolem $\mathcal{A}(\boldsymbol{x})$ a nazýváme jej *hodnotou zobrazení $\mathcal{A}$ v $\boldsymbol{x}$* nebo také *obrazem prvku $\boldsymbol{x}$*. V tomto kontextu se prvku $\boldsymbol{x}$ říká *vzor*. Je-li $M \subseteq L_1$, pak definujeme

$$\mathcal{A}(M) = \big\{\boldsymbol{y} \in L_2;\ \exists \boldsymbol{x} \in M \text{ tak, že } \mathcal{A}(\boldsymbol{x}) = \boldsymbol{y}\big\}.$$

4.3. Příklad. Pro ilustraci uvedeme příklady některých zobrazení:

(1) Funkce $f : \mathbf{R} \to \mathbf{R}$, která každému $x \in \mathbf{R}$ přiřadí $\sin(x) \in \mathbf{R}$ je speciální případ zobrazení.
(2) Zobrazení $\mathcal{A}_2$ z množiny diferencovatelných funkcí do množiny funkcí, které každé funkci přiřadí její derivaci. Tj. $\mathcal{A}_2(f) = f'$.

(3) Zobrazení $\mathcal{A}_3$ z množiny orientovaných úseček do množiny orientovaných úseček, které každému vektoru přiřadí jeho „stín“ na pevně zvolené rovině procházející počátkem.
(4) Zobrazení $\mathcal{A}_4$ z množiny spojitých funkcí do množiny reálných čísel, které každé spojité funkci přiřadí hodnotu určitého integrálu této funkce od nuly do jedné. Tedy $\mathcal{A}_4(f) = \int_0^1 f(x)\mathrm{d}x$.
(5) Zobrazení $\mathcal{A}_5$ z množiny funkcí do množiny nekonečných posloupností, které každé funkci f přiřadí nekonečnou posloupnost $f(1), f(2), f(3), \ldots$
(6) Zobrazení $\mathcal{A}_6$ z množiny posloupností do množiny funkcí, které každé posloupnosti c_1, c_2, c_3, přiřadí po částech konstantní funkci, která je nulová na $(-\infty, 1)$ a $f(x) = c_i$ pro $x \in \langle i, i+1)$.
(7) Zobrazení $\mathcal{C}_B$ z množiny orientovaných úseček U_O do množiny uspořádaných trojic $\mathbf{R}^3$, které každé úsečce přidělí její souřadnice vzhledem k pevně zvolené uspořádané bázi (B).

4.4. Definice. Nechť L_1 a L_2 jsou libovolné množiny a uvažujme $\mathcal{A}\colon L_1 \to L_2$. Pokud platí $\mathcal{A}(L_1) = L_2$, říkáme, že $\mathcal{A}$ je zobrazení z množiny L_1 *na množinu* L_2 (nebo říkáme, že zobrazení je *surjektivní*).

4.5. Poznámka. Zobrazení $\mathcal{A}$ z množiny L_1 na množinu L_2 je speciální případ zobrazení z množiny L_1 do množiny L_2 (všimneme si rozdílnosti slůvek „do“ a „na“). Může se stát, že existují prvky $\boldsymbol{y} \in L_2$, pro které neexistuje žádný prvek $\boldsymbol{x} \in L_1$, který by splňoval $\mathcal{A}(\boldsymbol{x}) = \boldsymbol{y}$.

V takovém případě zobrazení $\mathcal{A}$ není „na“ množinu L_2, je jenom „do“ množiny L_2. Lidově řečeno, množina L_2 je v takovém případě „větší“, než množina všech obrazů zobrazení $\mathcal{A}$.

4.6. Definice. Nechť L_1 a L_2 jsou libovolné množiny a uvažujme $\mathcal{A}\colon L_1 \to L_2$. Zobrazení $\mathcal{A}$ je *prosté* (*injektivní*), pokud pro každé dva prvky $\boldsymbol{x}_1 \in L_1$, $\boldsymbol{x}_2 \in L_1$, $\boldsymbol{x}_1 \neq \boldsymbol{x}_2$ platí $\mathcal{A}(\boldsymbol{x}_1) \neq \mathcal{A}(\boldsymbol{x}_2)$. Je-li zobrazení prosté i „na“ množinu, říkáme mu *bijektivní* zobrazení.

4.7. Příklad. Zobrazení (4), (5) a (7) z příkladu ?? jsou „na“ množinu (surjektivní). Ostatní zobrazení v tomto příkladu nejsou „na“ množinu. Zobrazení (6) a (7) jsou zobrazení prostá (injektivní). Ostatní zobrazení v příkladu ?? nejsou prostá. Zobrazení (7) je prosté i „na“, tedy je to bijektivní zobrazení.

4.8. Definice.* Nechť L_1 a L_2 jsou lineární prostory, $\mathcal{A}\colon L_1 \to L_2$ je zobrazení z L_1 do L_2. Zobrazení $\mathcal{A}$ nazýváme *lineárním zobrazením*, pokud pro všechna $\boldsymbol{x} \in L_1$, $\boldsymbol{y} \in L_1$, $\alpha \in \mathbf{R}$ platí

$$\begin{aligned} &(1) \quad \mathcal{A}(\boldsymbol{x}+\boldsymbol{y}) = \mathcal{A}(\boldsymbol{x}) + \mathcal{A}(\boldsymbol{y}),\\ &(2) \quad \mathcal{A}(\alpha \cdot \boldsymbol{x}) = \alpha \cdot \mathcal{A}(\boldsymbol{x}). \end{aligned}$$

4.9. Poznámka.* Lineární zobrazení „zachovává“ operace sčítání a násobení konstantou. Sečteme-li dva prvky z L_1 a výsledek převedeme prostřednictvím lineárního zobrazení do L_2, výjde totéž, jako kdybychom nejprve jednotlivé prvky převedli prostřednictvím zobrazení do

L_2 a tam je sečetli. Všimneme si, že první operace „+“ ve vlastnosti (1) je sčítáním definovaným na lineárním prostoru L_1, zatímco druhá operace „+“ v této vlastnosti je sčítáním definovaným na lineárním prostoru L_2. Tato dvě sčítání mohou být definována zcela rozdílným způsobem na zcela rozdílných lineárních prostorech. Podobně ve vlastnosti (2) je první operace „$\cdot$“ násobkem definovaným na L_1, zatímco druhá operace „$\cdot$“ je násobek definovaný na L_2.

4.10. Věta. Pro lineární zobrazení $\mathcal{A}\colon L_1 \to L_2$ platí $\mathcal{A}(\boldsymbol{o}_1) = \boldsymbol{o}_2$, kde $\boldsymbol{o}_1$ je nulový vektor lineárního prostoru L_1 a $\boldsymbol{o}_2$ je nulový vektor lineárního prostoru L_2.

Důkaz. Podle vlastnosti (7) definice ?? je $\boldsymbol{o}_1 = 0\,\boldsymbol{x}$, kde $\boldsymbol{x} \in L_1$. Podle vlastnosti (2) definice ?? je $\mathcal{A}(\boldsymbol{o}_1) = \mathcal{A}(0\,\boldsymbol{x}) = 0\,\mathcal{A}(\boldsymbol{x}) = \boldsymbol{o}_2$.

4.11. Příklad. Prozkoumáme linearitu zobrazení z příkladu ??.

Zobrazení (1) není lineární, protože $\sin(\pi/2+\pi/2) = \sin(\pi) = 0 \neq \sin(\pi/2)+\sin(\pi/2) = 2$. Zobrazení $\mathcal{A}_2$ je lineární, protože $(f+g)' = f'+g'$ a $(\alpha f)' = \alpha f$. Zobrazení $\mathcal{A}_3$ je lineární za předpokladu, že světlo dopadá na rovinu z nekonečně vzdáleného zdroje, tj. paprsky jsou rovnoběžné. Dále musí mít svůj stín (ze světla z protisměru) i vektory, které jsou „schovány za rovinou“. Sčítání a násobení konstantou provádíme v tomto příkladě geometricky v souladu s příkladem ??. Skutečně platí, že stín součtu je součet stínů a alfa násobek stínu je stín alfa násobku. Načrtněte si obrázek a najděte v něm odpovídající podobné trojúhelníky.

Zobrazení $\mathcal{A}_4$ je lineární: $\int(f(x)+g(x))\mathrm{d}x = \int f(x)\mathrm{d}x + \int g(x)\mathrm{d}x$ a $\int(\alpha f(x))\mathrm{d}x = \alpha\int f(x)\mathrm{d}x$. Zobrazení $\mathcal{A}_5$ je lineární, protože $(f+g)(i) = f(i)+g(i)$ a $(\alpha f)(i) = \alpha(f(i))$ pro všechna přirozená i. Na prostoru L_1 v tomto případě sčítáme funkce, na prostoru L_2 sčítáme nekonečné posloupnosti. Zobrazení $\mathcal{A}_6$ je lineární, protože $(c_1, c_2 \dots) + (d_1, d_2 \dots) = (c_1+d_1, c_2+d_2 \dots)$ a obraz této posloupnosti je roven součtu obrazů jednotlivých posloupností $(c_1, c_2 \dots)$ a $(d_1, d_2 \dots)$. Na L_2 sčítáme funkce. Také platí $\alpha(c_1, c_2 \dots) = (\alpha c_1, \alpha c_2, \dots)$ a obraz této posloupnosti je α-násobkem obrazu posloupnosti $(c_1, c_2 \dots)$. Linearitu zobrazení $\mathcal{C}_B$, které každému vektoru přiřadí souřadnice, dokážeme v tomto textu později.

4.12. Příklad. Ověříme, zda je zobrazení $\mathcal{A}\colon \mathbf{R}^2 \to \mathbf{R}^3$, definované vzorcem

$$\mathcal{A}(x_1, x_2) = (x_1 + 2x_2,\ -x_2,\ 2x_1 - 3x_2),$$

lineární. Poznamenejme, že jsme v uvedeném vzorci vynechali jednu kulatou závorku, jako se to obvykle u zobrazení definovaných na $\mathbf{R}^n$ dělá, tj. místo abychom psali $\mathcal{A}\big((x_1, x_2)\big)$, píšeme stručně $\mathcal{A}(x_1, x_2)$.

Ověříme vlastnosti (1) a (2) z definice ??:

$$
\begin{aligned}
(1)\quad & \mathcal{A}\big((x_1,x_2)+(y_1,y_2)\big)=\mathcal{A}(x_1+y_1,x_2+y_2)=\\
&=\big(x_1+y_1+2(x_2+y_2),-(x_2+y_2),2(x_1+y_1)-3(x_2+y_2)\big)=\\
&=(x_1+2x_2,-x_2,2x_1-3x_2)+(y_1+2y_2,-y_2,2y_1-3y_2)=\mathcal{A}(x_1,x_2)+\mathcal{A}(y_1,y_2),\\
(2)\quad & \mathcal{A}\big(\alpha\,(x_1,x_2)\big)=\mathcal{A}(\alpha\,x_1,\alpha\,x_2)=(\alpha\,x_1+2\alpha\,x_2,-\alpha\,x_2,2\alpha\,x_1-3\alpha\,x_2)=\\
&=\alpha\,(x_1+2x_2,-x_2,2x_1-3x_2)=\alpha\,\mathcal{A}(x_1,x_2).
\end{aligned}
$$

4.13. Příklad. Zobrazení $\mathcal{A}\colon \mathbf{R}^4\to\mathbf{R}^3$ definované předpisem $\mathcal{A}(x_1,x_2,x_3,x_4)=(x_2+x_3,x_3+3,2x_1)$ není lineární, protože $\mathcal{A}(0,0,0,0)=(0,3,0)$ a to není nulový vektor v $\mathbf{R}^3$. Podle věty ?? musí každé lineární zobrazení zobrazit nulový vektor na nulový vektor.

Pilnější čtenáři si zkusí ověřit, že $\mathcal{A}$ není lineární, přímo z definice ??.

4.14. Poznámka. Podmínka věty ??, že $\mathcal{A}(\boldsymbol{o}_1)=\boldsymbol{o}_2$, je nutná podmínka linearity zobrazení, ale není to podmínka postačující. Například $\sin(0)=0$, ale zobrazení $\sin:\mathbf{R}\to\mathbf{R}$ není lineární.

4.15. Příklad. Nechť $\mathbf{R}$ je lineární prostor z příkladu ?? a $\mathbf{R}^+$ je lineární prostor z příkladu ??. Uvažujme zobrazení $\exp:\mathbf{R}\to\mathbf{R}^+$, které každému reálnému číslu x přiřadí hodnotu e^x. Toto

zobrazení je lineární. Skutečně:

$$\exp(x+y) = \exp x \cdot \exp y = (\exp x) \oplus (\exp y), \qquad \exp(\alpha x) = (\exp x)^{\alpha} = \alpha \odot (\exp x).$$

Vidíme, že linearita zobrazení závisí nejen na způsobu přiřazení hodnoty zobrazením, ale také na operacích $+$ a $\cdot$, které jsou definovány na jednotlivých lineárních prostorech L_1 a L_2. Zjevně zobrazení $\exp : \mathbf{R} \to \mathbf{R}$ lineární není, protože $\exp(0) = 1$, tj. nulový prvek se nezobrazí na nulový prvek.

4.16. Věta (princip superpozice). Nechť L_1 a L_2 jsou lineární prostory. Zobrazení $\mathcal{A} : L_1 \to L_2$ je lineární právě tehdy, když pro všechna $\boldsymbol{x} \in L_1$, $\boldsymbol{y} \in L_1$, $\alpha \in \mathbf{R}$, $\beta \in \mathbf{R}$ platí

$$\mathcal{A}(\alpha\, \boldsymbol{x} + \beta\, \boldsymbol{y}) = \alpha\, \mathcal{A}(\boldsymbol{x}) + \beta\, \mathcal{A}(\boldsymbol{y}). \tag{4.1}$$

Důkaz. Nejprve předpokládejme, že pro zobrazení $\mathcal{A} : L_1 \to L_2$ platí (4.1) pro všechna $\boldsymbol{x}, \boldsymbol{y} \in L_1$ a $\alpha, \beta \in \mathbf{R}$. Dokážeme, že $\mathcal{A}$ je lineární, tj. že platí (1) a (2) z definice ??. Pokud zvolíme $\alpha = \beta = 1$, plyne z (4.1) vlastnost (1) a pokud volíme $\beta = 0$, plyne z (4.1) vlastnost (2).

Nechť nyní $\mathcal{A} : L_1 \to L_2$ je lineární. Platí

$$\mathcal{A}(\alpha\, \boldsymbol{x} + \beta\, \boldsymbol{y}) \overset{(1)}{=} \mathcal{A}(\alpha\, \boldsymbol{x}) + \mathcal{A}(\beta\, \boldsymbol{y}) \overset{(2)}{=} \alpha\, \mathcal{A}(\boldsymbol{x}) + \beta\, \mathcal{A}(\boldsymbol{y}).$$

Nad rovnítky jsme uvedli, kterou vlastnost jsme zrovna použili.

4.17. Poznámka. Opakovaným použitím principu superpozice (nebo formálně matematickou indukcí) lze snadno dokázat, že $\mathcal{A}\colon L_1 \to L_2$ je lineární právě tehdy, když pro všechna $n \in \mathbf{N}$, $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \in L_1$, $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbf{R}$ platí

$$\mathcal{A}(\alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_n \boldsymbol{x}_n) = \alpha_1 \mathcal{A}(\boldsymbol{x}_1) + \alpha_2 \mathcal{A}(\boldsymbol{x}_2) + \cdots + \alpha_n \mathcal{A}(\boldsymbol{x}_n). \tag{4.2}$$

4.18. Věta. Nechť $\mathcal{A}\colon L_1 \to L_2$ je lineární zobrazení, $M \subseteq L_1$. Pak $\mathcal{A}\big(\langle M\rangle\big) = \big\langle \mathcal{A}(M)\big\rangle$.

Důkaz. Nechť $\boldsymbol{y} \in \mathcal{A}\big(\langle M\rangle\big)$. Pak existuje vektor $\boldsymbol{x} \in \langle M\rangle$ takový, že $\mathcal{A}(\boldsymbol{x}) = \boldsymbol{y}$. Protože $\boldsymbol{x} \in \langle M\rangle$, existuje podle definice lineárního obalu konečně mnoho $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_i \in M$ takových, že $\boldsymbol{x}$ je lineární kombinací těchto vektorů. Protože $\mathcal{A}$ je lineární, máme podle (4.2)

$$\boldsymbol{y} = \mathcal{A}(\boldsymbol{x}) = \mathcal{A}(\alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_n \boldsymbol{x}_n) = \alpha_1 \mathcal{A}(\boldsymbol{x}_1) + \alpha_2 \mathcal{A}(\boldsymbol{x}_2) + \cdots + \alpha_n \mathcal{A}(\boldsymbol{x}_n).$$

Z tohoto zápisu je patrné, že $\boldsymbol{y} \in \big\langle \mathcal{A}(M)\big\rangle$.

Nechť nyní obráceně $\boldsymbol{y} \in \big\langle \mathcal{A}(M)\big\rangle$. Z definice lineárního obalu plyne, že existuje konečně mnoho $\boldsymbol{y}_i \in \mathcal{A}(M)$ takových, že $\boldsymbol{y}$ je lineární kombinací těchto vektorů. Pro každý vektor $\boldsymbol{y}_i$ existuje vektor $\boldsymbol{x}_i \in M$ takový, že $\mathcal{A}(\boldsymbol{x}_i) = \boldsymbol{y}_i$. Máme tedy

$$\boldsymbol{y} = \beta_1 \boldsymbol{y}_1 + \beta_2 \boldsymbol{y}_2 + \cdots + \beta_m \boldsymbol{y}_m = \beta_1 \mathcal{A}(\boldsymbol{x}_1) + \cdots + \beta_m \mathcal{A}(\boldsymbol{x}_m) = \mathcal{A}(\beta_1 \boldsymbol{x}_1 + \beta_2 \boldsymbol{x}_2 + \cdots + \beta_m \boldsymbol{x}_m) = \mathcal{A}$$

Je tedy $\boldsymbol{x} \in \langle M\rangle$ a protože $\boldsymbol{y} = \mathcal{A}(\boldsymbol{x})$, je též $\boldsymbol{y} \in \mathcal{A}\big(\langle M\rangle\big)$.

4.19. Poznámka. Věta ?? má tento důsledek: Je-li $M \subseteq L_1$ lineární podprostor v L_1, pak $\mathcal{A}(M)$ je lineární podprostor v L_2. Stačí si uvědomit platnost věty ??. Lineární zobrazení nám tedy převádí podprostory na podprostory. Speciálně $\mathcal{A}(L_1)$ je podprostor v L_2, který nazýváme *prostor obrazů*.

4.20. Definice.* Nechť L_1, L_2 jsou lineární prostory, $\boldsymbol{o}_2$ je nulový vektor v lineárním prostoru L_2 a $\mathcal{A}\colon L_1 \to L_2$ je lineární zobrazení. Množinu

$$\operatorname{Ker}\mathcal{A} = \{\boldsymbol{x} \in L_1;\ \mathcal{A}(\boldsymbol{x}) = \boldsymbol{o}_2\}.$$

nazýváme *jádrem lineárního zobrazení* $\mathcal{A}$.

4.21. Věta. Jádro lineárního zobrazení $\mathcal{A}\colon L_1 \to L_2$ tvoří lineární podprostor lineárního prostoru L_1

Důkaz. Pro $\boldsymbol{x}, \boldsymbol{y} \in \operatorname{Ker}\mathcal{A}$ a $\alpha \in \mathbf{R}$ platí:

$\mathcal{A}(\boldsymbol{x}) = \boldsymbol{o}_2$, $\mathcal{A}(\boldsymbol{x}) = \boldsymbol{o}_2$, takže $\mathcal{A}(\boldsymbol{x}+\boldsymbol{y}) = \mathcal{A}(\boldsymbol{x}) + \mathcal{A}(\boldsymbol{x}) = \boldsymbol{o}_2 + \boldsymbol{o}_2 = \boldsymbol{o}_2$, neboli $\boldsymbol{x}+\boldsymbol{y} \in \operatorname{Ker}$

dále $\mathcal{A}(\alpha\boldsymbol{x}) = \alpha\mathcal{A}(\boldsymbol{x}) = \alpha\boldsymbol{o}_2 = \boldsymbol{o}_2$, takže také $\alpha\boldsymbol{x} \in \operatorname{Ker}\mathcal{A}$.

4.22. Příklad. Najdeme jádro zobrazení $\mathcal{A}$ z příkladu ??. Podle definice ?? je

$$\operatorname{Ker}\mathcal{A} = \big\{(x_1, x_2);\ \mathcal{A}(x_1, x_2) = (0,0,0)\big\} = \big\{(x_1, x_2);\ (x_1 + 2x_2, -x_2, 2x_1 - 3x_2) = (0,0,0)\big\}.$$

Protože uspořádané trojice se rovnají, když se rovnají odpovídající složky, musí čísla x_1, x_2 splňovat soustavu lineárních rovnic

$$\begin{aligned} x_1 + 2x_2 &= 0 \\ -x_2 &= 0 \\ 2x_1 - 3x_2 &= 0 \end{aligned}$$

ze které plyne, že $x_1 = 0$ a $x_2 = 0$. Takže $\operatorname{Ker}\mathcal{A} = \big\{(0,0)\big\}$.

4.23. Příklad. Uvedeme si jádra lineárních zobrazení z příkladu ??.

$\operatorname{Ker}\mathcal{A}_2$ je roven množině všech funkcí, které jsou konstantní. Právě tyto funkce se totiž zobrazí pomocí derivace na nulovou funkci.

$\operatorname{Ker}\mathcal{A}_3$ je roven množině všech orientovaných úseček, které leží na přímce procházející počátkem, která je rovnoběžná s paprsky světla. Skutečně, tyto vektory mají nulový stín.

$\operatorname{Ker}\mathcal{A}_4$ obsahuje všechny funkce f, pro které je $\int_0^1 f(x)\mathrm{d}x = 0$.

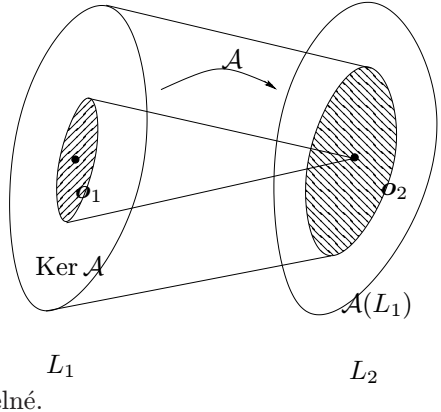
$\operatorname{Ker}\mathcal{A}_5$ obsahuje všechny funkce f, které mají nulovou hodnotu ve všech přirozených číslech. Hodnoty v ostatních reálných číslech mohou mít libovolné.

$\operatorname{Ker} \mathcal{A}_6 = \{(0,0,0,\ldots)\}$. Tento prostor obsahuje jen nulový vektor lineárního prostoru nekonečných posloupností.

Jediný vektor, který má nulové souřadnice, je nulový vektor (úsečka, která začíná i končí v bodě O). Proto i zobrazení (7) má ve svém jádru jen nulový vektor.

4.24. Definice.* *Defekt lineárního zobrazení* $\mathcal{A}: L_1 \to L_2$ je definován, jako $\dim \operatorname{Ker} \mathcal{A}$ a *hodnost lineárního zobrazení* $\mathcal{A}$ je definována jako $\dim \mathcal{A}(L_1)$. Defekt $\mathcal{A}$ značíme $\operatorname{def} \mathcal{A}$ a hodnost $\mathcal{A}$ značíme $\operatorname{hod} \mathcal{A}$. Je tedy

$$\operatorname{def} \mathcal{A} = \dim \operatorname{Ker} \mathcal{A},$$
$$\operatorname{hod} \mathcal{A} = \dim \mathcal{A}(L_1).$$



4.25. Poznámka. Později ukážeme, že defekt zobrazení udává zhruba řečeno „vzdálenost“ zobrazení od ideálního prostého zobrazení. Jak moc je zobrazení $\mathcal{A}$ „defektní“ souvisí také s tím, kolik informace, které dovedeme v prostoru L_1 rozlišit, se stává po aplikaci zobrazení $\mathcal{A}$ v prostoru L_2 nerozlišitelné.

4.26. Příklad. Podíváme se na defekty a hodnosti lineárních zobrazení z příkladu ??.

$\operatorname{def}\mathcal{A}_2 = \dim\operatorname{Ker}\mathcal{A}_2 = \dim\{c\cdot 1;\, c\in\mathbf{R}\} = \dim\langle 1\rangle = 1$. Protože $\mathcal{A}_2(L_1)$ obsahuje jistě (kromě dalších funkcí) všechny polynomy, má tento prostor nekonečnou dimenzi, tedy $\operatorname{hod}\mathcal{A}_2 = \infty$.

$\operatorname{def}\mathcal{A}_3 = \dim\operatorname{Ker}\mathcal{A}_3 = \dim\{\boldsymbol{u};\, \boldsymbol{u}$ leží na společné přímce$\} = 1$. Protože $\mathcal{A}_3(U_O)$ obsahuje množinu všech vektorů, které leží v rovině, kam se promítají stíny, je dimenze tohoto prostoru 2, neboli $\operatorname{hod}\mathcal{A}_3 = 2$. Zobrazení $\mathcal{A}_3$ se například používá v počítačové grafice, když je třeba 3D scénu zobrazit na stínítko monitoru. Rovnost $\operatorname{def}\mathcal{A}_3 = 1$ říká, že tímto zobrazením ztrácíme informace z jedné dimenze.

$\operatorname{def}\mathcal{A}_4 = \infty$, protože $\operatorname{Ker}\mathcal{A}_4$ obsahuje například funkce $(x-1/2), (x-1/2)^3, (x-1/2)^5, \ldots$ a těch je nekonečně mnoho a jsou lineárně nezávislé. Protože dále $\mathcal{A}_4(L_1) = \mathbf{R}$, je $\operatorname{hod}\mathcal{A}_4 = 1$.

$\operatorname{def}\mathcal{A}_5 = \infty$, protože $\operatorname{Ker}\mathcal{A}_5$ obsahuje také funkce, které jsou rovny polynomům až na to, že na přirozených číslech jsou rovny nule. Tyto funkce jsou sice nespojité, ale L_1 obsahuje všechny funkce, tedy i nespojité funkce. $\operatorname{hod}\mathcal{A}_5 = \infty$, protože množina $\mathcal{A}(L_1)$ obsahuje všechny nekonečné posloupnosti, jmenovitě tedy $(1,0,0,\ldots), (0,1,0,\ldots), \ldots$ a ty jsou lineárně nezávislé a je jich nekonečně mnoho.

$\operatorname{def}\mathcal{A}_6 = 0$, protože $\operatorname{Ker}\mathcal{A}_6 = \{\boldsymbol{o}_1\}$. $\operatorname{hod}\mathcal{A}_6 = \infty$, protože například obrazy následujících posloupností $(1,0,0,\ldots), (0,1,0,\ldots), \ldots$ jsou lineárně nezávislé.

$\operatorname{def}\mathcal{C}_B = \dim\{\boldsymbol{o}_1\} = 0$, $\operatorname{hod}\mathcal{C}_B = \dim\mathbf{R}^3 = 3$.

4.27. Příklad. Zobrazení $\mathcal{A}\colon \mathbf{R}^2 \to \mathbf{R}^3$, $\mathcal{A}(x_1,x_2) = (x_1+2x_2, -x_2, 2x_1-3x_2)$ z příkladu ?? má defekt roven nule. V příkladu ?? jsme totiž ukázali, že $\operatorname{Ker}\mathcal{A} = \{\boldsymbol{o}_1\}$. Spočítáme ještě

hod $\mathcal{A}$:

$$\operatorname{hod}\mathcal{A} = \dim \mathcal{A}(L_1) = \dim \mathcal{A}(\langle(1,0),(0,1)\rangle) = \dim\langle \mathcal{A}(1,0), \mathcal{A}(0,1)\rangle = \dim\langle(1,0,2),(2,-1,-3)\rangle$$

4.28. Věta.* Nechť $\mathcal{A}\colon L_1 \to L_2$ je lineární zobrazení. Pak $\operatorname{def}\mathcal{A} + \operatorname{hod}\mathcal{A} = \dim L_1$

Důkaz (pro hloubavé čtenáře). Nechť nejprve jsou def $\mathcal{A}$ i hod $\mathcal{A}$ konečné. Označme $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$ bázi lineárního podprostoru $\operatorname{Ker}\mathcal{A}$ a $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m$ bázi lineárního podprostoru $\mathcal{A}(L_1)$. Ke každému vektoru $\boldsymbol{c}_i$ existuje vektor $\boldsymbol{c}'_i \in L_1$ takový, že $\mathcal{A}(\boldsymbol{c}'_i) = \boldsymbol{c}_i$. K jednomu vektoru $\boldsymbol{c}_i$ může existovat více vektorů $\boldsymbol{c}'_i$ uvedené vlastnosti, v takovém případě je jedno, který vybereme. Dokážeme, že $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k, \boldsymbol{c}'_1, \boldsymbol{c}'_2, \ldots, \boldsymbol{c}'_m\}$ tvoří bázi lineárního prostoru L_1. Dokazovaný vzorec pak plyne z toho, že $\dim L_1$ je rovna počtu prvků báze, tedy $\dim L_1 = k + m$, přitom $\operatorname{def}\mathcal{A} = k$ a $\operatorname{hod}\mathcal{A} = m$.

Proč je množina $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k, \boldsymbol{c}'_1, \boldsymbol{c}'_2, \ldots, \boldsymbol{c}'_m\}$ lineárně nezávislá?

$$\begin{aligned}
&\boldsymbol{o}_1 = \alpha_1\,\boldsymbol{b}_1 + \alpha_2\,\boldsymbol{b}_2 + \cdots + \alpha_k\,\boldsymbol{b}_k + \beta_1\,\boldsymbol{c}'_1 + \beta_2\,\boldsymbol{c}'_2 + \cdots + \beta_k\,\boldsymbol{c}'_k,\\
\text{takže:}\quad &\boldsymbol{o}_2 = \mathcal{A}(\boldsymbol{o}_1) = \mathcal{A}(\alpha_1\,\boldsymbol{b}_1 + \alpha_2\,\boldsymbol{b}_2 + \cdots + \alpha_k\,\boldsymbol{b}_k + \beta_1\,\boldsymbol{c}'_1 + \beta_2\,\boldsymbol{c}'_2 + \cdots + \beta_k\,\boldsymbol{c}'_k,) =\\
&\quad = \mathcal{A}(\alpha_1\,\boldsymbol{b}_1 + \alpha_2\,\boldsymbol{b}_2 + \cdots + \alpha_k\,\boldsymbol{b}_k) + \beta_1\mathcal{A}(\boldsymbol{c}'_1) + \beta_2\mathcal{A}(\boldsymbol{c}'_2) + \cdots \beta_m\mathcal{A}(\boldsymbol{c}'_m) =\\
&\quad = \beta_1\mathcal{A}(\boldsymbol{c}'_1) + \beta_2\mathcal{A}(\boldsymbol{c}'_2) + \cdots \beta_m\mathcal{A}(\boldsymbol{c}'_m) = \beta_1\,\boldsymbol{c}_1 + \beta_2\,\boldsymbol{c}_2 + \cdots + \beta_m\,\boldsymbol{c}_m.
\end{aligned}$$

Využili jsme vztahu $\mathcal{A}(\alpha_1\,\boldsymbol{b}_1 + \alpha_2\,\boldsymbol{b}_2 + \cdots + \alpha_k\,\boldsymbol{b}_k) = \boldsymbol{o}_2$, který je důsledkem faktu, že tato lineární kombinace leží v $\operatorname{Ker}\mathcal{A}$. Protože $\{\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m\}$ je báze, je lineárně nezávislá, takže

$\beta_i = 0$ pro všechny $i \in \{1, 2, \ldots, m\}$ (pouze triviální lineární kombinace báze je rovna nulovému vektoru). Dosazením tohoto poznatku do původního vztahu máme $\boldsymbol{o}_1 = \alpha_1\,\boldsymbol{b}_1 + \alpha_2\,\boldsymbol{b}_2 + \cdots + \alpha_k\,\boldsymbol{b}_k$. Protože $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k\}$ je báze, musí $\alpha_i = 0$ pro všechny $i \in \{1, 2, \ldots, k\}$. Takže pouze triviální lineární kombinace množiny vektorů $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k, \boldsymbol{c}'_1, \boldsymbol{c}'_2, \ldots, \boldsymbol{c}'_m\}$ je rovna nulovému vektoru, je tedy tato množina lineárně nezávislá.

Proč je $\langle \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k, \boldsymbol{c}'_1, \boldsymbol{c}'_2, \ldots, \boldsymbol{c}'_m \rangle = L_1$? Je třeba ukázat, že každý vektor $\boldsymbol{x}$ lze zapsat jako lineární kombinaci vektorů z $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k, \boldsymbol{c}'_1, \boldsymbol{c}'_2, \ldots, \boldsymbol{c}'_m\}$. Existují koeficienty β_i tak, že

$$\mathcal{A}(\boldsymbol{x}) = \beta_1\,\boldsymbol{c}_1 + \beta_2\,\boldsymbol{c}_2 + \cdots + \beta_m\,\boldsymbol{c}_m,$$

protože $\{\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m\}$ je báze $\mathcal{A}(L_2)$. Dále platí

$$\mathcal{A}(\boldsymbol{x} - \beta_1\,\boldsymbol{c}'_1 + \beta_2\,\boldsymbol{c}'_2 + \cdots + \beta_m\,\boldsymbol{c}'_m) = \mathcal{A}(\boldsymbol{x}) - (\beta_1\,\boldsymbol{c}_1 + \beta_2\,\boldsymbol{c}_2 + \cdots + \beta_m\,\boldsymbol{c}_m) = \mathcal{A}(\boldsymbol{x}) - \mathcal{A}(\boldsymbol{x}) = \boldsymbol{o}_2,$$

takže vektor $\boldsymbol{x} - \beta_1\,\boldsymbol{c}'_1 + \beta_2\,\boldsymbol{c}'_2 + \cdots + \beta_m\,\boldsymbol{c}'_m$ leží v $\operatorname{Ker}\mathcal{A}$ a lze jej vyjádřit jako lineární kombinaci báze lineárního podprostoru $\operatorname{Ker}\mathcal{A}$. Je tedy

$$\boldsymbol{x} - \beta_1\,\boldsymbol{c}'_1 + \beta_2\,\boldsymbol{c}'_2 + \cdots + \beta_m\,\boldsymbol{c}'_m = \alpha_1\,\boldsymbol{b}_1 + \alpha_2\,\boldsymbol{b}_2 + \cdots + \alpha_k\,\boldsymbol{b}_k$$

a po přičtení $\beta_1\,\boldsymbol{c}'_1 + \beta_2\,\boldsymbol{c}'_2 + \cdots + \beta_m\,\boldsymbol{c}'_m$ k oběma stranám rovnosti máme $\boldsymbol{x}$ vyjádřený jako lineární kombinaci vektorů $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k, \boldsymbol{c}'_1, \boldsymbol{c}'_2, \ldots, \boldsymbol{c}'_m$.

Je-li $\operatorname{def}\mathcal{A} = \infty$, musí být též $\dim \mathbf{L}_1 = \infty$, protože $\operatorname{Ker}\mathcal{A}$ má nekonečnou dimezi a je podprostorem lineárního prostoru L_1. Nechť konečně $\operatorname{hod}\mathcal{A} = \infty$. Pro spor předpokládejme, že $\dim L_1$ je konečná. Nechť $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k\}$ je báze L_1. Platí $\mathcal{A}(L_1) = \mathcal{A}(\langle \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k\rangle) = \langle \mathcal{A}(\boldsymbol{b}_1), \mathcal{A}(\boldsymbol{b}_2), \ldots \mathcal{A}(\boldsymbol{b}_k)\rangle$. Podle věty ?? tento obal nemůže obsahovat lineárně nezávislou množinu s větším počtem prvků než k, což je spor s tím, že $\operatorname{hod}\mathcal{A} = \infty$.

4.29. Příklad. Povšimneme si, že věta $\operatorname{def}\mathcal{A} + \operatorname{hod}\mathcal{A} = \dim L_1$ „funguje“ ve všech příkladech lineárních zobrazení uvedených v příkladu ??. (2): $1 + \infty = \infty$, (3): $1 + 2 = 3$, (4): $\infty + 1 = \infty$, (5): $\infty + \infty = \infty$, (6): $0 + \infty = \infty$, (7) $0 + 3 = 3$. Zobrazení z příkladu ?? rovněž splňuje $0 + 2 = 2$.

4.30. Věta. Nechť $\mathcal{A}\colon L_1 \to L_2$ je lineární zobrazení. Pak $\operatorname{def}\mathcal{A} = 0$ právě tehdy, když $\mathcal{A}$ je prosté.

Důkaz. Nechť $\operatorname{def}\mathcal{A} = 0$ a $\boldsymbol{x}, \boldsymbol{y} \in L_1$, $\boldsymbol{x} \neq \boldsymbol{y}$. Pro spor předpokládejme, že $\mathcal{A}(\boldsymbol{x}) = \mathcal{A}(\boldsymbol{y})$, takže $\mathcal{A}(\boldsymbol{x}) - \mathcal{A}(\boldsymbol{y}) = \boldsymbol{o}_2$, takže $\mathcal{A}(\boldsymbol{x} - \boldsymbol{y}) = \boldsymbol{o}_2$. To znamená, že $\boldsymbol{x} - \boldsymbol{y} \in \operatorname{Ker}\mathcal{A}$, ale podle předpokladu víme, že $\boldsymbol{x} - \boldsymbol{y} \neq \boldsymbol{o}_1$ a současně $\operatorname{Ker}\mathcal{A} = \{\boldsymbol{o}_1\}$. Spor.

Nechť nyní $\mathcal{A}$ je prosté. Víme, $\mathcal{A}(\boldsymbol{o}_1) = \mathcal{A}(\boldsymbol{o}_2)$. Protože je $\mathcal{A}$ prosté, je $\boldsymbol{o}_1$ jediný vektor, který se zobrazí na $\boldsymbol{o}_2$, takže $\operatorname{Ker}\mathcal{A} = \{\boldsymbol{o}_1\}$.

4.31. Věta. Nechť $\mathcal{A}: L_1 \to L_2$ je lineární zobrazení, $M \subseteq L_1$ je lineárně závislá množina v L_1. Pak je $\mathcal{A}(M)$ lineárně závislá množina v L_2.

Důkaz. Je-li M lineárně závislá, pak konečná pomnožina $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k\} \subseteq M$ je lineárně závislá. Takže platí

$$\alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_n \boldsymbol{x}_n = \boldsymbol{o}_1,$$

přičemž aspoň jedno α_i je nenulové. Zobrazením obou stran rovnice a z principu superpozice dostáváme:

$$\mathcal{A}(\alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_n \boldsymbol{x}_n) = \alpha_1 \mathcal{A}(\boldsymbol{x}_1) + \alpha_2 \mathcal{A}(\boldsymbol{x}_2) + \cdots + \alpha_n \mathcal{A}(\boldsymbol{x}_n) = \boldsymbol{o}_2,$$

přitom stále jedno α_i je nenulové. Takže vektory $\{\mathcal{A}(\boldsymbol{x}_1), \mathcal{A}(\boldsymbol{x}_2), \ldots, \mathcal{A}(\boldsymbol{x}_n)\} \subseteq \mathcal{A}(M)$ jsou lineárně závislé, takže i $\mathcal{A}(M)$ je lineárně závislá množina.

4.32. Poznámka. Lineární zobrazení nemusí lineárně nezávislou množinu N zobrazit na množinu lineárně nezávislou. Například nenulová konstantní funkce se zobrazí při použití zobrazení $\mathcal{A}_2$ z příkladu ?? (derivace) na nulovou funkci, tedy na nulový vektor v L_2, který je lineárně závislý. Vzorem byla ale nenulová funkce, tedy lineárně nezávislý vektor.

V předchozím textu jsme ukázali, že všechny ostatní „vlastnosti linearity“ (lineární podprostor, lineární obal, lineární závislost) se při lineárním zobrazení nemění. V jakém případě se nemění lineární nezávislost ukazuje následující věta.

4.33. Věta. Lineární zobrazení $\mathcal{A}$ zobrazuje lineárně nezávislé množiny vzorů na lineárně nezávislé množiny obrazů právě tehdy, když $\mathcal{A}$ je prosté zobrazení.

Důkaz. Nechť nejprve $\mathcal{A}(N)$ je lineárně nezávislá pro všechny lineárně nezávislé množiny N. Dokážeme, že $\mathcal{A}$ je prosté zobrazení. Volme vektory $\boldsymbol{x}, \boldsymbol{y} \in L_1$, $\boldsymbol{x} \neq \boldsymbol{y}$. Potřebujeme dokázat $\mathcal{A}(\boldsymbol{x}) \neq \mathcal{A}(\boldsymbol{y})$. Zvolme $N = \{\boldsymbol{x} - \boldsymbol{y}\}$, tj. N je nezávislá. Pak $\mathcal{A}(N) = \{\mathcal{A}(\boldsymbol{x} - \boldsymbol{y})\}$ je podle předpokladu lineárně nezávislá, tedy $\mathcal{A}(\boldsymbol{x}-\boldsymbol{y}) \neq \boldsymbol{o}_2$. Z linearity zobrazení je $\boldsymbol{o}_2 \neq \mathcal{A}(\boldsymbol{x}-\boldsymbol{y}) = \mathcal{A}(\boldsymbol{x}) - \mathcal{A}(\boldsymbol{y})$, neboli $\mathcal{A}(\boldsymbol{x}) \neq \mathcal{A}(\boldsymbol{y})$.

Obráceně, předpokládejme, že $\mathcal{A}$ je prosté a N je lineárně nezávislá množina. Pro spor budeme předpokládat, že $\mathcal{A}(N)$ je lineárně závislá. Pak musí existovat konečně mnoho $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, $ N, pro které lze najít nenulové α_i tak, že

$$\alpha_1\mathcal{A}(\boldsymbol{x}_1) + \alpha_2\mathcal{A}(\boldsymbol{x}_2) + \ldots + \alpha_n\mathcal{A}(\boldsymbol{x}_n) = \boldsymbol{o}_2$$

Podle principu superpozice je

$$\alpha_1\mathcal{A}(\boldsymbol{x}_1) + \alpha_2\mathcal{A}(\boldsymbol{x}_2) + \ldots + \alpha_n\mathcal{A}(\boldsymbol{x}_n) = \mathcal{A}(\alpha_1\boldsymbol{x}_1 + \alpha_2\boldsymbol{x}_2 + \ldots + \alpha_n\boldsymbol{x}_n) = \boldsymbol{o}_2$$

takže $\alpha_1\boldsymbol{x}_1 + \alpha_2\boldsymbol{x}_2 + \ldots + \alpha_n\boldsymbol{x}_n \in \operatorname{Ker}\mathcal{A}$. Protože je $\mathcal{A}$ prosté, je podle věty ?? $\operatorname{Ker}\mathcal{A} = \{\boldsymbol{o}_1\}$. Takže $\alpha_1\boldsymbol{x}_1 + \alpha_2\boldsymbol{x}_2 + \ldots + \alpha_n\boldsymbol{x}_n = \boldsymbol{o}_1$. Připomeňme, že $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k\}$ je podmnožinou N, takže tyto vektory jsou podle věty ?? lineárně nezávislé. Dále připomeňme, že ve vztahu $\alpha_1\boldsymbol{x}_1 + \alpha_2\boldsymbol{x}_2 + \ldots + \alpha_n\boldsymbol{x}_n = \boldsymbol{o}_1$ existuje nenulové α_i. Dostáváme spor.

4.34. Poznámka.* Předchozí věty nám zaručují, že zobrazení, které je lineární a prosté, zobrazí vešekré „lineární skutečnosti“, které můžeme zkoumat v lineárním prostoru L_1 (závislost, nezávislost, podprostory, lineární obaly, báze, dimenze), bez ztráty informace do lineárního prostoru L_2. Pokud je lineární prostor L_2 volen tak, že se tam tyto skutečnosti pohodlněji zkoumají, stojí za to převést pomocí „vhodného lineárního zobrazení“ problém z L_1 do L_2 a tam jej podrobit zkoumání. Takovým vhodným lineárním zobrazením je zobrazení, které vektorům přiřazuje souřadnice. To říká následující věta.

4.35. Věta.* Nechť L je lineární prostor, $\dim L = n$ a nechť (B) je uspořádaná báze prostoru L. Pak je zobrazení $\mathcal{C}_B \colon L \to \mathbf{R}^n$, které každému vektoru $\boldsymbol{x} \in L$ přiřadí jeho souřadnice vzhledem k uspořádané bázi (B), zobrazením lineárním, prostým a na $\mathbf{R}^n$.

Důkaz. Věta ?? říká, že každému vektoru $\boldsymbol{x}$ lze jednoznačně přiřadit uspořádanou n-tici souřadnic vzhledem k uspořádané bázi (B), takže $\mathcal{C}_B$ je zobrazení z L do $\mathbf{R}^n$.

Proč je linární? Nechť $\mathcal{C}_B(\boldsymbol{x}) = (\alpha_1, \alpha_2, \dots, \alpha_n)$, $\mathcal{C}_B(\boldsymbol{y}) = (\beta_1, \beta_2, \dots, \beta_n)$. Pro větší názornost operace v L budeme značit $\oplus$, $\odot$, zatímco operace v $\mathbf{R}^n$ definované v příkladu ?? stejně jako běžné operace v $\mathbf{R}$ označíme $+$ a $\cdot$. Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n)$. Pro vektory vektory $\boldsymbol{x}$ a $\boldsymbol{y}$ platí

$$\boldsymbol{x} = \alpha_1 \odot \boldsymbol{b}_1 \oplus \alpha_2 \odot \boldsymbol{b}_2 \oplus \cdots \oplus \alpha_n \odot \boldsymbol{b}_n, \qquad \boldsymbol{y} = \beta_1 \odot \boldsymbol{b}_1 \oplus \beta_2 \odot \boldsymbol{b}_2 \oplus \cdots \oplus \beta_n \odot \boldsymbol{b}_n.$$

Po sečtení těchto rovností a po vynásobení první rovnosti číslem $\gamma \in \mathbf{R}$ dostáváme

$$\begin{aligned}\boldsymbol{x} \oplus \boldsymbol{y} &= (\alpha_1 + \beta_1)\odot\boldsymbol{b}_1 \oplus (\alpha_2 + \beta_2)\odot\boldsymbol{b}_2 \oplus \cdots \oplus (\alpha_n + \beta_n)\odot\boldsymbol{b}_n,\\ \gamma\odot\boldsymbol{x} &= (\gamma \cdot \alpha_1)\odot\boldsymbol{b}_1 \oplus (\gamma \cdot \alpha_2)\odot\boldsymbol{b}_2 \oplus \cdots \oplus (\gamma \cdot \alpha_n)\odot\boldsymbol{b}_n.\end{aligned}$$

Protože souřadnice vektoru vzhledem k bázi jsou určeny jednoznačně, z uvedených rovností plyne, že $\mathcal{C}_B(\boldsymbol{x} \oplus \boldsymbol{y}) = \mathcal{C}_B(\boldsymbol{x}) + \mathcal{C}_B(\boldsymbol{y})$, $\mathcal{C}_B(\gamma\odot\boldsymbol{x}) = \gamma \cdot \mathcal{C}_B(\boldsymbol{x})$. Zobrazení $\mathcal{C}_B$ je tedy lineární.

Hledejme nyní $\operatorname{Ker}\mathcal{C}_B$. Protože $\boldsymbol{o} = 0 \cdot \boldsymbol{b}_1 \oplus 0 \cdot \boldsymbol{b}_2 \oplus \cdots \oplus 0 \cdot \boldsymbol{b}_n$ a nenulovému vektoru se triviální lineární kombinace rovnat nemůže, je $\operatorname{Ker}\mathcal{C}_B = \{\boldsymbol{o}\}$, neboli $\operatorname{def}\mathcal{C}_B = 0$. Z věty ?? plyne, že $\mathcal{C}_B$ je prosté zobrazení.

Protože ke každému prvku $\boldsymbol{a} \in \mathbf{R}^n$, $\boldsymbol{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ existuje $\boldsymbol{x} \in L$, pro který $\mathcal{C}_B(\boldsymbol{x}) = \boldsymbol{a}$ (stačí volit $\boldsymbol{x} = \alpha_1\odot\boldsymbol{b}_1 \oplus \alpha_2\odot\boldsymbol{b}_2 \oplus \cdots \oplus \alpha_n\odot\boldsymbol{b}_n$), je $\mathcal{C}_B(L) = \mathbf{R}^n$. Zobrazení $\mathcal{C}_B$ je tedy zobrazením z L „na“ $\mathbf{R}^n$. Je $\operatorname{hod}\mathcal{C}_B = \dim\mathbf{R}^n = n$.

4.36. Definice.* Lineární zobrazení $\mathcal{A}\colon L_1 \to L_2$, které je prosté a na L_2 se nazývá *izomorfismus*. Existuje-li izomorfismus $\mathcal{A}\colon L_1 \to L_2$, říkáme, že prostory L_1, L_2 *jsou izomorfní*, nebo že L_1 *je izomorfní* s L_2, resp. L_2 *je izomorfní* s L_1.

4.37. Poznámka. Je zřejmé, že zobrazení $\mathcal{A}\colon L_1 \to L_2$, které je prosté a na L_2, má tu vlastnost, že každému $\boldsymbol{y} \in L_2$ lze jednoznačně najít $\boldsymbol{x} \in L_1$ tak, že $\mathcal{A}(\boldsymbol{x}) = \boldsymbol{y}$. Skutečně, pro daný obraz $\boldsymbol{y} \in L_2$ lze vzor $\boldsymbol{x} \in L_1$ najít, protože $\mathcal{A}$ je „na“ L_2. Přiřazení je jednoznačné, protože

$\mathcal{A}$ je prosté. Toto „zpětné zobrazení“ z L_2 do L_1 se nazývá *zobrazení inverzní* k zobrazení $\mathcal{A}$ a značíme je $\mathcal{A}^{-1}$. Později v této kapitole tento pojem zavedeme přesněji a ukážeme, že inverzní zobrazení k lineárnímu zobrazení je rovněž zobrazení lineární. Takže inverzní zobrazení k izomorfismu existuje a je rovněž izomorfizmus. To je důvod, proč v definici ?? izomorfních prostorů se nerozlišuje mezi tvrzeními „L_1 je izomorfní s L_2“ a „L_2 je izomorfní s L_1“.

4.38. Věta.* Každý lineární prostor L, pro který je $\dim L = n$, je izomorfní s lineárním prostorem $\mathbf{R}^n$.

Důkaz. Hledaným izomorfismem jsou například souřadnice vzhledem k bázi, viz větu ??.

4.39. Poznámka. Předchozí věta má v lineární algebře zásadní význam. Potřebujeme-li zkoumat „vlastnosti linearity“ na libovolném lineárním prostoru konečné dimenze, stačí nám pomocí izomorfizmu souřadnic zkoumat tyto vlastnosti v lineárním prostoru $\mathbf{R}^n$. V tomto lineárním prostoru sčítáme a násobíme konstantou po složkách, tedy pracujeme s reálnými čísly. Algoritmy, které řeší „otázky linearity“ v $\mathbf{R}^n$ jsou tedy založeny na numerických výpočtech. Složky vektorů z $\mathbf{R}^n$ budeme v rámci těchto algorimů často zapisovat do řádků pod sebe, čímž vznikají tabulky čísel, kterým říkáme *matice*. V následujících kapitolách zaměříme tedy pozornost na lineární prostor $\mathbf{R}^n$ a naučíme se pracovat s maticemi.

4.40. Příklad. Nechť P je lineární podprostor lineárního prostoru U_O orientovaných úseček, které všechny leží v rovině papíru tohoto textu (nebo v rovině stínítka obrazovky, pokud to nějaký nešťastník čte z obrazovky počítače) a všechny začínají v bodě O na obrázku. V P jsou dány dva vektory $\boldsymbol{u}$ a $\boldsymbol{v}$ (viz stejný obrázek). Kdybychom chtěli tyto vektory například sečíst v lineárním podprostoru P, musíme použít pravítko a kružítko, neboť sčítání je v tomto linárním prostoru definováno geometricky (viz příklad ??). Můžeme ale problém „sečtení těchto dvou vektorů“ přenést pomocí izomorfismu souřadnic do lineárního prostoru $\mathbf{R}^2$. Volbu báze a nalezení souřadnic vidíme na obrázku. Souřadnice vektoru $\boldsymbol{u}$ vzhledem k bázi $(\boldsymbol{b}_1, \boldsymbol{b}_2)$ jsou rovny $(1, 2)$ a souřadnice vektoru $\boldsymbol{v}$ vzhledem ke stejné bázi jsou $(5, 1)$. V lineárním prostoru $\mathbf{R}^2$ můžeme provést součet: $(1, 2) + (5, 1) = (6, 3)$. Tento výpočet jsme provedli *numericky*. Konečně je možné výsledek v $\mathbf{R}^2$ převést zpět do původního lineárního podprostoru P pomocí inverzního izomorfismu. V lineárním podprostoru P pak výsledek narýsujeme.

Nebo se můžeme ptát, zda vektory $\boldsymbol{u}$ a $\boldsymbol{v}$ jsou lineárně nezávislé v U_O. To zjistíme „pohledem na ně“, že totiž neleží ve společné přímce. Vektory $\boldsymbol{u}$ a $\boldsymbol{v}$ jsou lineárně nezávislé právě tehdy, když jsou lineárně nezávislé jejich souřadnice v $\mathbf{R}^2$. To zaručuje izomorfismus souřadnic. Souřadnice těchto vektorů můžeme zapsat do řádků matice:

$$\mathbf{A} = \begin{pmatrix} 2 & 1 \\ 1 & 5 \end{pmatrix}$$

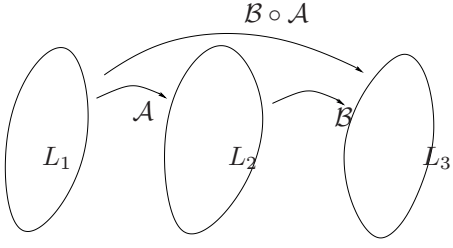
Ukážeme v následujících kapitolách, že lineární nezávislost řádků takové matice lze ověřit výpočtem determinantu matice $\mathbf{A}$ a ověřením, že je tento determinant nenulový. V $\mathbf{R}^n$ tedy jsme schopni otázky linearity zkoumat numericky (pomocí algoritmů založených na počítání s čísly). Tento *numerický výpočet* pak odpoví díky izomorfismu souřadnic i na *geometrickou otázku*, zda třeba vektory leží či neleží v jedné přímce.

4.41. Poznámka. Isomorfizmus souřadnic nám umožňuje si každý vektor lineárního prostoru konečné dimenze představit jako uspořádanou n-tici, třebaže ten vektor ve skutečnosti je popsán jinak. Třeba v případě geometrického prostoru dimenze 3 orientovaných úseček můžeme při představě vektoru myšlenkově „přepínat“ mezi orientovanou úsečkou a uspořádanou trojicí podle potřeby. Nebo zkoumání lineární závislosti a nezávislosti polynomů nejvýše n-tého stupně můžeme převést na zkoumání závislosti či nezávislosti uspořádaných $(n+1)$-tic jeho koeficientů. Zobrazení, které polynomu přiřadí souřadnice vzhledem k uspořádané bázi $(1, x, x^2, \ldots, x^n)$, je totiž izomorfismus.

4.42. Poznámka. V závěru této kapitoly zavedeme složené zobrazení, inverzní zobrazení a uvedeme jejich vlastnosti. K lineárním zobrazením se pak vrátíme ještě v kapitole ??, kde odhalíme mnoho dalších vlastností zejména v souvislosti s tím, že mezi zobrazeními lineárních prostorů konečné dimenze a maticemi čísel je úzká souvislost.

4.43. Definice. Nechť $\mathcal{A}\colon L_1 \to L_2$ a $\mathcal{B}\colon L_2 \to L_3$ jsou zobrazení. Symbolem $\mathcal{B}\circ\mathcal{A}\colon L_1 \to L_3$ označujeme *složené zobrazení*, které je definováno předpisem $(\mathcal{B}\circ\mathcal{A})(\boldsymbol{x}) = \mathcal{B}\big(\mathcal{A}(\boldsymbol{x})\big)$, $\forall \boldsymbol{x} \in L_1$.

4.44. Poznámka. Symbol $\circ$ pro skládání zobrazení čteme „zprava doleva“. To znamená, že ve složeném zobrazení $\mathcal{B}\circ\mathcal{A}$ zpracuje vstupní hodnotu $\boldsymbol{x}$ nejprve zobrazení $\mathcal{A}$ a vytvoří „mezivýsledek“ $\mathcal{A}(x)$, který je dále zpracován zobrazením $\mathcal{B}$. Důvod tohoto „arabského čtení“ vyplývá ze skutečnosti, že vstupní hodnotu $\boldsymbol{x}$ klademe do závorky *vpravo* od symbolu zobrazení, takže $(\mathcal{B}\circ\mathcal{A})(\boldsymbol{x}) = \mathcal{B}\big(\mathcal{A}(\boldsymbol{x})\big)$. Je třeba také upozornit na to, že literatura v tomto značení není jednotná.



4.45. Věta. Nechť $\mathcal{A}\colon L_1 \to L_2$ a $\mathcal{B}\colon L_2 \to L_3$ jsou lineární zobrazení. Pak je lineární též složené zobrazení $(\mathcal{B}\circ\mathcal{A})\colon L_1 \to L_3$.

Důkaz. Nechť $\boldsymbol{x} \in L_1$, $\boldsymbol{y} \in L_1$, $\alpha \in \mathbf{R}$.

$$(\mathcal{B} \circ \mathcal{A})(\boldsymbol{x}+\boldsymbol{y}) = \mathcal{B}\big(\mathcal{A}(\boldsymbol{x}+\boldsymbol{y})\big) = \mathcal{B}\big(\mathcal{A}(\boldsymbol{x}) + \mathcal{A}(\boldsymbol{y})\big) = \mathcal{B}\big(\mathcal{A}(\boldsymbol{x})\big) + \mathcal{B}\big(\mathcal{A}(\boldsymbol{y})\big) = (\mathcal{B} \circ \mathcal{A})(\boldsymbol{x}) + (\mathcal{B} \circ$$
$$(\mathcal{B} \circ \mathcal{A})(\alpha\,\boldsymbol{x}) = \mathcal{B}\big(\mathcal{A}(\alpha\,\boldsymbol{x})\big) = \mathcal{B}\big(\alpha\,\mathcal{A}(\boldsymbol{x})\big) = \alpha\,\mathcal{B}\big(\mathcal{A}(\boldsymbol{x})\big) = \alpha\,(\mathcal{B} \circ \mathcal{A})(\boldsymbol{x}).$$

4.46. Definice. *Identické zobrazení* je zobrazení $\mathcal{I}\colon L \to L$, které je definováno předpisem $\mathcal{I}(\boldsymbol{x}) = \boldsymbol{x}$. Stručně nazýváme zobrazení $\mathcal{I}$ *identitou*. Nechť $\mathcal{A}\colon L_1 \to L_2$ je prosté zobrazení. Pak definujeme *inverzní zobrazení* $\mathcal{A}^{-1}\colon \mathcal{A}(L_1) \to L_1$ jako takové zobrazení, které splňuje $\mathcal{A}^{-1} \circ \mathcal{A} = \mathcal{I}$, kde $\mathcal{I}\colon L_1 \to L_1$ je identita.

4.47. Věta. Je-li $\mathcal{A}\colon L_1 \to L_2$ prosté, pak existuje právě jedno inverzní zobrazení $\mathcal{A}^{-1}\colon \mathcal{A}(L_1) \to L_1$.

Důkaz. Pro každý prvek $\boldsymbol{y} \in \mathcal{A}(L_1)$ existuje právě jeden prvek $\boldsymbol{x} \in L_1$ takový, že $\mathcal{A}(\boldsymbol{x}) = \boldsymbol{y}$. To plyne přímo z definice ?? prostého zobrazení. Definujeme $\mathcal{A}^{-1}(\boldsymbol{y}) = \boldsymbol{x}$. Vidíme, že $\mathcal{A}^{-1} \circ \mathcal{A}$ je identita.

4.48. Věta. Je-li L lineární prostor, pak identita $\mathcal{I}\colon L \to L$ je lineární. Je-li $\mathcal{A}\colon L_1 \to L_2$ lineární a prosté zobrazení, pak též $\mathcal{A}^{-1}\colon \mathcal{A}(L_1) \to L_1$ je lineární.

Důkaz. Identita je zcela zřejmě lineární. Ověříme linearitu zobrazení $\mathcal{A}^{-1}$. Počítejme $\mathcal{A}^{-1}(\boldsymbol{x}+\boldsymbol{y})$ pro $\boldsymbol{x} \in \mathcal{A}(L_1)$, $\boldsymbol{y} \in \mathcal{A}(L_1)$. Podle poznámky ?? je $\mathcal{A}(L_1)$ lineární podprostor, takže $\boldsymbol{x}+\boldsymbol{y} \in \mathcal{A}(L_1)$. Protože $\mathcal{A}$ je prosté, existuje právě jeden vektor $\boldsymbol{a} \in L_1$ a právě jeden vektor $\boldsymbol{b} \in L_1$ tak, že $\mathcal{A}(\boldsymbol{a}) = \boldsymbol{x}$, $\mathcal{A}(\boldsymbol{b}) = \boldsymbol{y}$. Platí tedy $\mathcal{A}^{-1}(\boldsymbol{x}) = \boldsymbol{a}$, $\mathcal{A}^{-1}(\boldsymbol{y}) = \boldsymbol{b}$. Protože $\mathcal{A}$ je lineární, je $\mathcal{A}(\boldsymbol{a}+\boldsymbol{b}) = \boldsymbol{x}+\boldsymbol{y}$, neboli

$$\mathcal{A}^{-1}(\boldsymbol{x}+\boldsymbol{y}) = \boldsymbol{a}+\boldsymbol{b} = \mathcal{A}^{-1}(\boldsymbol{x}) + \mathcal{A}^{-1}(\boldsymbol{y}).$$

Protože $\mathcal{A}$ je lineární, platí pro $\alpha \in \mathbf{R}$, že $\mathcal{A}(\alpha\,\boldsymbol{a}) = \alpha\,\boldsymbol{x}$, neboli $\mathcal{A}^{-1}(\alpha\,\boldsymbol{x}) = \alpha\,\boldsymbol{a} = \alpha\,\mathcal{A}^{-1}(\boldsymbol{x})$.

4.49. Věta. Nechť $\mathcal{A}\colon L_1 \to L_2$ je izomorfismus. Pak je inverzní zobrazení $\mathcal{A}^{-1}\colon L_2 \to L_1$ rovněž izomorfismus.

Důkaz. Izomorfismus je zobrazení, které je lineární, prosté a „na“.

Že je $\mathcal{A}^{-1}$ definováno na celém L_2 plyne z toho, že $\mathcal{A}$ je „na“ L_2, neboli $\mathcal{A}(L_1) = L_2$.

Že je $\mathcal{A}^{-1}$ lineární plyne z věty ??.

Že je $\mathcal{A}^{-1}$ prosté plyne z toho, že je $\mathcal{A}$ zobrazení. Dvěma různým prvkům $\boldsymbol{x} \in L_2$, $\boldsymbol{y} \in L_2$ musejí odpovídat různé prvky $\boldsymbol{a} \in L_1$ a $\boldsymbol{b} \in L_1$ takové, že $\mathcal{A}(\boldsymbol{a}) = \boldsymbol{x}$, $\mathcal{A}(\boldsymbol{b}) = \boldsymbol{y}$. Kdyby mělo platit $\boldsymbol{a} = \boldsymbol{b}$, okamžitě vidíme, že zobrazení $\mathcal{A}$ nemůže splňovat $\mathcal{A}(\boldsymbol{a}) = \boldsymbol{x} \neq \boldsymbol{y} = \mathcal{A}(\boldsymbol{b}) = \mathcal{A}(\boldsymbol{a})$.

Ukážeme, že $\mathcal{A}^{-1}$ je „na“ L_1. Každý prvek $\boldsymbol{a} \in L_1$ je zobrazením $\mathcal{A}$ převeden na nějaký prvek $\mathcal{A}(\boldsymbol{a}) = \boldsymbol{x} \in L_2$. Jinými slovy neexistuje prvek $\boldsymbol{a} \in L_1$, který by neměl svůj protějšek $\mathcal{A}(\boldsymbol{a}) = \boldsymbol{x} \in L_2$.

4.50. Věta.* Složení dvou izomorfismů je izomorfismus.

Důkaz. Uvažujme izomorfismy $\mathcal{A}\colon L_1 \to L_2$, $\mathcal{B}\colon L_2 \to L_3$. Dokážeme, že $\mathcal{B}\circ\mathcal{A}$ je izomorfismus.

$\mathcal{B}\circ\mathcal{A}$ je lineární díky větě ??. $\mathcal{B}\circ\mathcal{A}$ je prosté, protože $\mathcal{A}$ je prosté i $\mathcal{B}$ je prosté. Konečně $\mathcal{B}\circ\mathcal{A}$ je „na“ L_3, protože $\mathcal{B}\big(\mathcal{A}(L_1)\big) = \mathcal{B}(L_2) = L_3$.

4.51. Věta.* Každé dva lineární prostory stejné konečné dimenze jsou vzájemně izomorfní.

Důkaz. Nechť L_1, L_2 jsou lineární prostory, $\dim L_1 = \dim L_2 = n$. Pak existují podle věty ?? izomorfismy $\mathcal{A}\colon L_1 \to \mathbf{R}^n$ a $\mathcal{B}\colon L_2 \to \mathbf{R}^n$. Podle věty ?? je $\mathcal{B}^{-1}\colon \mathbf{R}^n \to L_2$ izomorfismus. Nakonec věta ?? říká, že $\mathcal{B}^{-1}\circ\mathcal{A}\colon L_1 \to L_2$ je izomorfismus.

4.52. Poznámka. Poslední věta zhruba říká, že je zbytečné při studiu vlastností lineárních prostorů konečné dimenze mezi nimi rozlišovat. Například polynomy nejvýše druhého stupně se chovají z hlediska „vlastností linearity“ stejně jako orientovné úsečky se společným počátkem a ty se chovají stejně jako uspořádané trojice reálných čísel. Pro lineární prostory nekonečné dimenze analogická věta neplatí.

4.53. Shrnutí. Zobrazení je lineární, pokud zobrazí součet vzorů na součet obrazů a alfanásobek vzoru na alfanásobek obrazu /??/, tedy pokud zobrazení „respektuje“ součet a

násobek. Tato vlastnost je ekvivalentní s principem superpozice, tj. lineární kombinace vzorů se zobrazí na lineární kombinaci obrazů se stejnými koeficienty /??/. Z té okamžitě plyne, že lineární obaly (neboli podprostory) vzorů se přenesou na lineární obaly (neboli podprostory) obrazů /??/.

Množinu všech vzorů, které se zobrazí na nulový vektor ve výstupním lineárním prostoru, označujeme symbolem Ker a jedná se o podprostor vstupního lineárního prostoru /??/. Dimenzi tohoto podprostoru říkáme defekt /??/. Hodnost zobrazení je dimenze podprostoru všech obrazů. Součet defektu a hodnosti je roven dimezi vstupního lineárního prostoru /??/.

Lineární zobrazení je prosté /??/ právě tehdy, když má nulový defekt /??/ což platí právě tehdy, když jsou všechny lineárně nezávislé množiny zobrazeny na lineárně nezávislé množiny /??/. Lineární zobrazení které je prosté, tedy zachová všechny lineární vztahy mezi vzory i v postoru obrazů (závislost, nezávislost, báze, dimenze, podprostory, obaly). Je-li takové zobrazení navíc „na“ prostor L_2, říkáme mu izomorfismus /??/.

Souřadnice vzhledem ke konečné uspořádané bázi zobrazují libovolný vektor na uspořádanou n-tici v $\mathbf{R}^n$ a je to izomorfismus /??/. Díky tomu jsou všechny lineární prostory dimenze n izomorfní s $\mathbf{R}^n$ /??/ a jsou izomorfní i sobě navzájem /??/. Při studiu linárních skutečností, které jsou důsledky axiomů linearity v definici ??, není tedy třeba rozlišovat mezi jednotlivými lineárními prostory stejné dimenze. Často se pomocí izomofismu souřadnic „přepneme“ do $\mathbf{R}^n$ a tam lineární problém řešíme numericky. K tomu budeme potřebovat umět dobře počítat s maticemi, a proto se této problematice věnují následující kapitoly.

5. Matice

S pojmem matice jsme se už seznámili v úvodu do Gaussovy eliminační metody. Nyní si definujeme pojem matice přesněji.

5.1. Definice. *Matice typu (m,n)* je tabulka reálných (nebo komplexních) čísel s m řádky a n sloupci. Číslo $a_{i,j}$ z i-tého řádku a j-tého sloupce této tabulky nazýváme *(i,j)-tý prvek* matice. Množinu všech matic typu (m,n) značíme $\mathbf{R}^{m,n}$, pokud má reálné prvky, a $\mathbf{C}^{m,n}$, pokud má komplexní prvky.

Matici $\mathbf{A} \in \mathbf{R}^{m,n}$ (nebo $\mathbf{A} \in \mathbf{C}^{m,n}$) zapisujeme takto:

$$\mathbf{A} = \begin{pmatrix} a_{1,1}, & a_{1,2}, & \dots, & a_{1,n} \\ a_{2,1}, & a_{2,2}, & \dots, & a_{2,n} \\ & & \vdots & \\ a_{m,1}, & a_{m,2}, & \dots, & a_{m,n} \end{pmatrix}$$

nebo zapíšeme jen stručně prvky matice $\mathbf{A}$:

$$\mathbf{A} = (a_{i,j}), \quad i \in \{1,2,\dots,m\},\ j \in \{1,2,\dots,n\}.$$

Matici, která má všechny prvky nulové, nazýváme *nulovou maticí*. Matici typu (m,n) nazýváme *čtvercovou maticí*, pokud $m = n$.

V následujícím textu budeme pracovat většinou s reálnými maticemi (tj. s maticemi z $\mathbf{R}^{m,n}$). Skoro všechny vlastnosti lze analogicky odvodit i pro matice komplexní.

5.2. Poznámka. Dvě matice *se rovnají*, pokud jsou stejného typu a všechny prvky jedné matice se rovnají odpovídajícím prvkům matice druhé. Přesněji, $\mathbf{A} = (a_{i,j}) \in \mathbf{R}^{m,n}$ se rovná matici $\mathbf{B} = (b_{i,j}) \in \mathbf{R}^{p,q}$, pokud $m = p$, $n = q$ a $a_{i,j} = b_{i,j}$ pro všechna $i \in \{1, 2, \ldots, m\}$, $j \in \{1, 2, \ldots, n\}$.

5.3. Definice. Nechť $\mathbf{A} = (a_{i,j}) \in \mathbf{R}^{m,n}$, $\mathbf{B} = (b_{i,j}) \in \mathbf{R}^{m,n}$. Matici $\mathbf{C} \in \mathbf{R}^{m,n}$ nazýváme *součtem matic* $\mathbf{A}, \mathbf{B}$ (značíme $\mathbf{C} = \mathbf{A} + \mathbf{B}$), pokud pro prvky matice $\mathbf{C} = (c_{i,j})$ platí $c_{i,j} = a_{i,j} + b_{i,j}$, $i \in \{1, 2, \ldots, m\}, j \in \{1, 2, \ldots, n\}$. Nechť $\alpha \in \mathbf{R}$. *α-násobek* matice $\mathbf{A}$ je matice $\alpha \cdot \mathbf{A} = (\alpha\, a_{i,j})$. Názorně:

$$\mathbf{A}+\mathbf{B} = \begin{pmatrix} a_{1,1}+b_{1,1}, & a_{1,2}+b_{1,2}, & \ldots, & a_{1,n}+b_{1,n} \\ a_{2,1}+b_{2,1}, & a_{2,2}+b_{2,2}, & \ldots, & a_{2,n}+b_{2,n} \\ & & \vdots & \\ a_{m,1}+b_{m,1}, & a_{m,2}+b_{m,2}, & \ldots, & a_{m,n}+b_{m,n} \end{pmatrix}, \quad \alpha\cdot\mathbf{A} = \begin{pmatrix} \alpha\, a_{1,1}, & \alpha\, a_{1,2}, & \ldots, & \alpha\, a_{1,n} \\ \alpha\, a_{2,1}, & \alpha\, a_{2,2}, & \ldots, & \alpha\, a_{2,n} \\ & & \vdots & \\ \alpha\, a_{m,1}, & \alpha\, a_{m,2}, & \ldots, & \alpha\, a_{m,n} \end{pmatrix}$$

5.4. Věta. Množina $\mathbf{R}^{m,n}$ tvoří se sčítáním matic a násobením matice reálným číslem podle definice ?? lineární prostor. Nulový vektor tohoto prostoru je nulová matice.

Důkaz. Důkaz si čtenář provede sám jako cvičení. Srovnejte s příklady ?? a ??.

5.5. Příklad. Množina

$$B = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

tvoří bázi lineárního prostoru $\mathbf{R}^{3,2}$.

Abychom to ukázali, ověříme lineární nezávislost B a dále vlastnost $\langle B \rangle = \mathbf{R}^{3,2}$. Nejprve ověříme lineární nezávislost. Položme lineární kombinaci prvků z B rovnu nulové matici:

$$\alpha \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} + \beta \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} + \gamma \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix} + \delta \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} + \varepsilon \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{pmatrix} + \zeta \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Odpovídající složky se musejí rovnat, což vede k šesti rovnicím: $\alpha = 0$, $\beta = 0$, $\gamma = 0$, $\delta = 0$, $\varepsilon = 0$, $\zeta = 0$. Jedině triviální lineární kombinace je rovna nulovému vektoru.

Ověříme nyní vlastnost (2) z definice ??. Nechť

$$\begin{pmatrix} a & b \\ c & d \\ e & f \end{pmatrix}$$

je nějaká matice z lineárního prostoru $\mathbf{R}^{3,2}$. Snadno zjistíme, že existuje lineární kombinace matic z množiny B, která je rovna této matici (stačí volit $\alpha = a$, $\beta = b$, $\gamma = c$, $\delta = d$, $\mu = e$, $\nu = f$). Tím jsme dokázali, že $\langle B \rangle = \mathbf{R}^{3,2}$ a B je tedy báze lineárního prostoru matic $\mathbf{R}^{3,2}$. Nazýváme ji *standardní bází*.

Dimenze lineárního prostoru $\mathbf{R}^{3,2}$ je počet prvků báze, je tedy rovna šesti.

5.6. Příklad. Platí $\dim \mathbf{R}^{m,n} = m \cdot n$. Analogicky jako v příkladu ?? lze totiž sestrojit bázi lineárního prostoru $\mathbf{R}^{m,n}$, která má $m \cdot n$ prvků.

5.7. Věta. Lineární prostor jednosloupcových matic $\mathbf{R}^{n,1}$ je izomorfní s lineárním prostorem $\mathbf{R}^n$. Lineární prostor jednořádkových matic $\mathbf{R}^{1,n}$ je rovněž izomorfní s lineárním prostorem $\mathbf{R}^n$.

Důkaz. Věta je důsledkem věty ??.

5.8. Poznámka. Mezi lineárním prostorem $\mathbf{R}^n$ a lineárním prostorem $\mathbf{R}^{n,1}$ budeme používat následující izomorfismus: složky vektoru z $\mathbf{R}^n$ napíšeme po řadě (místo do řádku) do sloupce. Vzhledem k tomuto izomorfismu často ztotožňujeme vektory z $\mathbf{R}^{n,1}$ s vektory z $\mathbf{R}^n$ a mluvíme o *sloupcových vektorech*. Analogicky vektory z $\mathbf{R}^{1,n}$ nazýváme *řádkové vektory* a také je ztotožňujeme s vektory z $\mathbf{R}^n$.

5.9. Poznámka. V následujícím textu si ukážeme, jaké vlastnosti má modifikace matice Gaussovou eliminační metodou. Na matici v tomto kontextu budeme pohlížet jako na matici řádkových vektorů kladených pod sebe. Přesněji, matice $\mathbf{R}^{m,n}$ obsahuje m řádkových vektorů (řádků matice), každý z nich je z lineárního prostoru $\mathbf{R}^{1,n}$. Tento lineární prostor podle poznámky ?? ztotožňujeme s lineárním prostorem $\mathbf{R}^n$.

5.10. Definice. Symbolem $\mathbf{A} \sim \mathbf{B}$ označujeme skutečnost, že matice $\mathbf{B}$ vznikla z matice $\mathbf{A}$ konečným počtem kroků podle Gaussovy eliminační metody. Za krok Gaussovy eliminační metody je považováno prohození řádků, pronásobení řádku nenulovou konstantou, přičtení násobku řádku k jinému, odstranění nulového řádku nebo přidání nulového řádku.

5.11. Věta. Relace „$\sim$“ je symetrická, tj. $\mathbf{A} \sim \mathbf{B}$ právě tehdy, když $\mathbf{B} \sim \mathbf{A}$.

Důkaz. Stačí ukázat, že po provedení jednoho kroku podle Gaussovy eliminační metody se lze pomocí dalších kroků podle Gaussovy eliminační metody vrátit k původní matici.

(1) Prohození dvou libovolných řádků mezi sebou. Stačí prohodit tytéž řádky mezi sebou ještě jednou a máme původní matici.

(2) Vynásobení jednoho řádku nenulovým reálným číslem α. Stačí vynásobit tento řádek číslem $1/\alpha$ a dostáváme původní matici.

(3) Přičtení α-násobku nějakého řádku $\boldsymbol{a}$ k řádku $\boldsymbol{b}$ (řádek $\boldsymbol{a}$ se v tomto kroku opisuje). K původní matici se pak vrátíme tak, že k právě změněnému řádku přičteme $(-\alpha)$-násobek řádku $\boldsymbol{a}$.

(4) Vynechání nebo přidání nulového řádku. Jestliže nulový řádek při přechodu k matici $\mathbf{B}$ vynecháme, tak jej zas při návratu k matici $\mathbf{A}$ přidáme. Pokud jej při přechodu k matici $\mathbf{B}$ přidáme, pak jej při návratu k matici $\mathbf{A}$ odebereme.

5.12. Poznámka. V některé literatuře se místo kroku (3) uvádí přičtení lineární kombinace ostatních řádků ke zvolenému řádku $\boldsymbol{b}$. Tento krok lze samozřejmě nahradit konečným opakováním kroku (3).

V jiné literaruře se někdy neuvádí prohození řádků jako samotný krok Gaussovy eliminační metody, protože tento krok lze (poněkud těžkopádně) provést opakovaným použitím kroku (3) a v závěru aplikací kroku (2):

$$\begin{pmatrix} \boldsymbol{a} \\ \boldsymbol{b} \end{pmatrix} \sim \begin{pmatrix} \boldsymbol{a} \\ \boldsymbol{a}+\boldsymbol{b} \end{pmatrix} \sim \begin{pmatrix} \boldsymbol{a}-(\boldsymbol{a}+\boldsymbol{b}) \\ \boldsymbol{a}+\boldsymbol{b} \end{pmatrix} = \begin{pmatrix} -\boldsymbol{b} \\ \boldsymbol{a}+\boldsymbol{b} \end{pmatrix} \sim \begin{pmatrix} -\boldsymbol{b} \\ \boldsymbol{a} \end{pmatrix} \sim \begin{pmatrix} \boldsymbol{b} \\ \boldsymbol{a} \end{pmatrix}.$$

5.13. Definice. Množinu všech řádků matice $\mathbf{A}$ značíme $\mathrm{r}\colon\mathbf{A}$. Lineární obal množiny všech řádků matice $\mathbf{A}$ je tedy označen symbolem $\langle \mathrm{r}\colon\mathbf{A}\rangle$.

5.14. Věta.* Je-li $\mathbf{A} \sim \mathbf{B}$, pak $\langle \mathrm{r}\colon\mathbf{A}\rangle = \langle \mathrm{r}\colon\mathbf{B}\rangle$. Jinými slovy: Gaussova eliminační metoda zachovává lineární obal řádků matice.

Důkaz. Dokážeme nejdříve pomocné tvrzení: jestliže $\mathbf{A}_1$ je matice, která vznikne z matice $\mathbf{A}$ jedním krokem podle Gaussovy eliminační metody, pak $\langle \mathrm{r}\colon\mathbf{A}_1\rangle \subseteq \langle \mathrm{r}\colon\mathbf{A}\rangle$.

Všechny řádky matice $\mathbf{A}_1$ lze zapsat jako lineární kombinaci řádků matice $\mathbf{A}$. Je přitom jedno, zda matice $\mathbf{A}_1$ vznikla prohozením řádků, pronásobením jednoho řádku nenulovým reálným číslem, přičtením násobku jednoho řádku k jinému, odebráním nebo přidáním nulového řádku. Platí tedy, že $\mathrm{r}\colon \mathbf{A}_1 \subseteq \langle \mathrm{r}\colon \mathbf{A}\rangle$. Podle věty ?? je $\langle \mathrm{r}\colon \mathbf{A}_1\rangle \subseteq \langle\langle \mathrm{r}\colon \mathbf{A}\rangle\rangle = \langle \mathrm{r}\colon \mathbf{A}\rangle$, takže $\langle \mathrm{r}\colon \mathbf{A}_1\rangle \subseteq \langle \mathrm{r}\colon \mathbf{A}\rangle$.

Pomocné tvrzení máme dokázáno. Pokud toto tvrzení uplatníme opakovaně (matice $\mathbf{B}$ vznikla z matice $\mathbf{A}$ po konečně mnoha krocích podle Gaussovy eliminační metody), máme výsledek $\langle \mathrm{r}\colon \mathbf{B}\rangle \subseteq \langle \mathrm{r}\colon \mathbf{A}\rangle$. Tvrzení dokazované věty nyní plyne ze symetrie relace „$\sim$“, tj. z věty ??.

Obrácené tvrzení k této větě „jestliže $\langle \mathrm{r}\colon \mathbf{A}\rangle = \langle \mathrm{r}\colon \mathbf{B}\rangle$, pak $\mathbf{A} \sim \mathbf{B}$“ dokážeme v odstavci ??.

5.15. Příklad. Řádky matice $\mathbf{A}$ i matice $\mathbf{B}$ uvedené níže mají podle věty ?? stejné lineární obaly. Tyto obaly tvoří podle věty ?? nějaký lineární podprostor lineárního prostoru $\mathbf{R}^5$.

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 4 & 7 \\ 1 & 1 & 1 & 3 & 4 \\ 3 & 5 & 7 & 8 & 12 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 4 & 3 \\ 0 & 1 & 2 & 1 & 1 \\ 0 & 1 & 2 & 4 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 4 & 3 \\ 0 & 0 & 0 & 3 & 2 \end{pmatrix} = \mathbf{B}$$

Snadno ověříme, že řádky matice $\mathbf{B}$ jsou lineárně nezávislé. Takže tyto řádky tvoří bázi lineárního podprostoru $\langle \mathrm{r}\colon \mathbf{B}\rangle = \langle \mathrm{r}\colon \mathbf{A}\rangle$. Vidíme tedy, že $\dim\langle \mathrm{r}\colon \mathbf{A}\rangle = 3$.

5.16. Definice.* *Hodnost matice* **A** značíme $\mathrm{hod}(\mathbf{A})$ a definujeme $\mathrm{hod}(\mathbf{A}) = \dim\langle \mathrm{r}\colon \mathbf{A}\rangle$.

5.17. Věta.* Je-li $\mathbf{A} \sim \mathbf{B}$, pak $\mathrm{hod}(\mathbf{A}) = \mathrm{hod}(\mathbf{B})$. Jinými slovy, Gaussova eliminační metoda nemění hodnost matice.

Důkaz. Věta je jednoduchým důsledkem věty ?? a definice ??.

5.18. Příklad. Matice **B** z příkladu ?? má zřejmě hodnost 3. Věta ?? nám zaručí, že i matice **A** z tohoto příkladu má hodnost 3.

5.19. Poznámka. Pozorný čtenář si jistě všiml, že v definici ?? jsme použili pojem „hodnost“ v kontextu lineárního zobrazení. Nyní jsme definovali hodnost matice. Zatím je rozumné toto vnímat jako dva různé pojmy, každý má svou definici. Také budeme definovat zvlášť inverzi matice, třebaže definice inverzního zobrazení už zazněla. V tuto chvíli se zaměříme pouze na vlastnosti matic, budeme hledat například algoritmy pro výpočet hodnosti matice a teoretické důsledky tohoto pojmu. Později budeme schopni sestavit izomorfismus mezi lineárním prostorem matic a lineárním prostorem lineárních zobrazení. Pak ukážeme, že uvedené pojmy se ve smyslu tohoto izomorfismu shodují.

5.20. Věta. Hodnost matice je maximální počet lineárně nezávislých řádků matice. Přesněji řečeno, hodnost je počet prvků největší lineárně nezávislé podmnožiny z množiny řádků matice.

Důkaz. Zkoumanou matici označím symbolem $\mathbf{A}$. Jsou-li řádky matice $\mathbf{A}$ lineárně nezávislé, položím $\mathbf{A} = \mathbf{A}'$, jinak odeberu postupně z $\mathbf{A}$ řádky, které jsou lineární kombinací ostatních, jako v příkladu ??. Po konečně mnoha odebráních vznikne matice $\mathbf{A}'$, která má lineárně nezávislé řádky a $\langle \mathrm{r}\colon \mathbf{A}\rangle = \langle \mathrm{r}\colon \mathbf{A}'\rangle$. Proces vzniku matice $\mathbf{A}'$ samozřejmě nemusí být jednoznačný. Ovšem řádky matice $\mathbf{A}'$ jsou v každém případě podmnožinou řádků matice $\mathbf{A}$, která je nejpočetnější z těch podmnožin, které jsou lineárně nezávislé. Řádky matice $\mathbf{A}'$ jsou totiž bází podprostoru $\langle \mathrm{r}\colon \mathbf{A}\rangle$ a kdyby existovala početnější lineárně nezávislá množina se stejným lineárním obalem, byla by také bází téhož podprostoru. To ale není možné, neboť dvě báze stejného lineárního (pod)prostoru mají podle věty ?? stejný počet prvků. Počet řádků matice $\mathbf{A}'$ je podle definice ?? roven hodnosti matice $\mathbf{A}$.

5.21. Poznámka. Často je hodnost matice definována jako maximální počet lineárně nezávislých řádků matice. Je ovšem potřeba si velmi pečlivě uvědomit, co slovo „maximální“ v této formulaci znamená, a je potřeba z takové definice umět dokázat větu ??.

5.22. Poznámka. Matice $\mathbf{B}$ v příkladu ?? je typickou ukázkou matice, která vznikne po ukončení přímého chodu Gaussovy eliminační metody. Jedná se o matici, ve které každý následující řádek má aspoň o jednu nulu v souvislé řadě nul (psané z leva) více, než řádek předchozí. Přitom matice neobsahuje nulové řádky. Takovým maticím říkáme schodovité (rozhraní mezi nulovými a nenulovými prvky tvoří schody).

5.23. Definice. Nechť matice $\mathbf{A}$ má řádky $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ a nechť žádný z nich není nulový. Nechť pro každé dva po sobě jdoucí řádky $\boldsymbol{a}_i$, $\boldsymbol{a}_{i+1}$ platí: má-li řádek $\boldsymbol{a}_i$ prvních k složek nulových, musí mít řádek $\boldsymbol{a}_{i+1}$ aspoň prvních $k+1$ složek nulových. Pak matici $\mathbf{A}$ nazýváme *schodovitou maticí*

5.24. Věta. Schodovitá matice má lineárně nezávislé řádky.

Důkaz. Lineární nezávislost ověříme z definice. Nechť matice $\mathbf{A}$ má řádky $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ a položme

$$\alpha_1 \boldsymbol{a}_1 + \alpha_2 \boldsymbol{a}_2 + \cdots + \alpha_n \boldsymbol{a}_n = \boldsymbol{o}.$$

Po převedení této rovnosti do soustavy rovnic odpovídají koeficienty jednotlivých rovnic sloupcům matice $\mathbf{A}$. Přitom tato soustava má vždy pouze triviální řešení. Z první nenulové rovnice totiž okamžitě plyne, že $\alpha_1 = 0$. Dosazením tohoto výsledku do ostatních rovnic dostaneme z některé z následujících rovnic výsledek $\alpha_2 = 0$. Znovu dosadíme. Tento postup opakujeme tak dlouho, dokud nedostaneme $\alpha_i = 0 \ \forall i \in \{1, \ldots, n\}$.

5.25. Věta.* Každou matici lze převést konečným počtem kroků Gaussovy eliminační metody na schodovitou matici.

Důkaz. Plyne z popisu přímého chodu Gaussovy eliminační metody, který je podrobně popsán v úvodní kapitole této učebnice.

5.26. Algoritmus. Předchozí věta nám společně s větou ?? dává záruky, že hodnost libovolné matice můžeme spočítat postupem, jaký jsme zvolili v příkladu ??. Tedy při výpočtu hodnosti matice $\mathbf{A}$ ji převedeme Gaussovou eliminační metodou na schodovitou matici $\mathbf{B}$ a v ní spočítáme počet nenulových řádků. Tento počet je roven hodnosti matice $\mathbf{B}$, protože její řádky jsou podle věty ?? lineárně nezávislé a tvoří tedy bázi svého lineárního obalu. Konečně $\operatorname{hod}\mathbf{A} = \operatorname{hod}\mathbf{B}$ díky větě ??.

5.27. Poznámka. Je zřejmé, že matice, která vznikne ze schodovité matice přehozením některých sloupců, má také lineárně nezávislé řádky. Nemusíme tedy nutně při hledání hodnosti matice vytvářet v jednotlivých etapách Gaussovy eliminační metody nulové prvky v těsně následujících sloupcích. Je-li to z nějakých důvodů výhodné, můžeme nejprve třeba vytvořit nuly pod prvním řádkem v osmém sloupci, pak opíšeme první a druhý řádek a vytváříme nuly ve třetím sloupci atd. Tento sofistikovanější postup doporučujeme ale použít jen tehdy, když jste důkladně seznámeni s klasickým postupem přímého chodu Gaussovy eliminační metody. Jinak může velmi snadno dojít k omylům.

5.28. Poznámka. Postup přímého chodu Gassovy eliminační metody podle poznámky ?? se může hodit ve dvou případech.

(1) Počítáme modelové příklady a snažíme se držet malých celých čísel. Přitom v prvním sloupci jsou nesoudělná čísla, což vede po eliminaci ke zbytečně velkým celým číslům.

Poznamenejme ale, že modelové příklady ze skript se v praxi většinou nevyskytují, takže podstatnější pro nás bude druhý případ využití.

(2) Při implementaci Gaussovy eliminační metody do počítače je vhodné se snažit minimalizovat zaokrouhlovací chyby. Ty mohou nežádoucím způsobem ovlivnit výsledek, pokud se například snažíme dělit číslem blízkým nule. Algoritmus by měl vyhledat optimální cestu při řešení Gaussovou eliminační metodou, aby se pokud možno vyhnul dělením takovými čísly.

5.29. Poznámka. Numerické vyhodnocování hodnosti matice v počítači má svá úskalí, která vyplývají z možných zaokrouhlovacích chyb. Hodnost je definována jednoznačně jako přirozené číslo (nebo nula), ale v praktických situacích se může stát, že toto číslo nelze zjistit zcela přesně. Podívejme se kupříkladu na tuto matici:

$$\mathbf{C} = \begin{pmatrix} 28{,}33333 & 11{,}33333 \\ 56{,}66667 & 22{,}66667 \end{pmatrix},$$

Kdybychom čísla v této matici považovali za zcela přesná, museli bychom říci, že $\hod(\mathbf{C}) = 2$. Pokud ale připustíme, že na posledním desetinném místě mohou být zaokrouhlovací chyby, pak nemáme jistotu, zda hodnost této matice není náhodou rovna jedné. Dobře implementovaný algoritmus Gaussovy eliminační metody v počítači by nás měl upozornit, je-li výsledek skutečně zaručen, nebo zda může dojít k závažným chybám, jako v této matici. Takovým maticím, jako matice $\mathbf{C}$ v tomto příkladě, říkáme *numericky nestabilní matice*.

Problematiku numerických metod v tuto chvíli opustíme, protože se věnujeme algebře.

5.30. Poznámka. Ve větě ?? jsme ukázali, že Gaussova eliminační metoda zachovává lineární obaly řádků matice a dále věta ?? ukazuje, že Gaussova eliminační metoda zachovává hodnost matice. Z toho plyne, že Gaussova eliminační metoda zachovává lineární závislost resp. nezávislost řádků. Přesněji to zformulujeme v následující větě ??. Nejprve ale potřebujeme dokázat následující větu.

5.31. Věta.* Matice $\mathbf{A}$ má lineárně nezávislé řádky právě tehdy, když její hodnost je rovna počtu jejích řádků.

Důkaz. Nechť má $\mathbf{A}$ lineárně nezávislé řádky. Pak tyto řádky tvoří bázi podprostoru $\langle \mathrm{r}\colon \mathbf{A}\rangle$, takže jejich počet je roven dimenzi tohoto podprostoru, neboli hodnosti matice $\mathbf{A}$. Nechť naopak má matice $\mathbf{A}$ lineárně závislé řádky. Pak je potřeba odebrat aspoň jeden řádek procesem popsaným v příkladu ?? tak, abychom dospěli k lineárně nezávislým řádkům, jejichž lineární obal je stejný jako $\langle \mathrm{r}\colon \mathbf{A}\rangle$. Tato lineárně nezávislá množina je bází podprostoru $\langle \mathrm{r}\colon \mathbf{A}\rangle$ a má méně prvků než je počet řádků matice $\mathbf{A}$. Hodnost matice $\mathbf{A}$ je tedy menší než počet jejích řádků.

5.32. Věta.* Nechť $\mathbf{A} \sim \mathbf{B}$ označuje, že matice $\mathbf{B}$ vznikla z $\mathbf{A}$ konečně mnoha kroky Gaussovy eliminační metody, přičemž krok odebrání nebo přidání nulového řádku není povolen. Pak řádky matice $\mathbf{A}$ jsou lineárně nezávislé právě tehdy, když jsou lineárně nezávislé řádky matice $\mathbf{B}$.

Důkaz. Protože jsme zakázali odebírání a přidávání řádků, má matice $\mathbf{A}$ stejný počet řádků jako matice $\mathbf{B}$. Podle věty ?? Gaussova eliminační metoda zachovává hodnost a je tedy v obou případech tato hodnost rovna počtu řádků nebo menší než počet řádků. Podle věty ?? to znamená, že v obou případech jsou řádky linárně nezávislé nebo jsou v obou případech lineárně závislé.

5.33. Algoritmus. Věta ?? nám dává návod, jak vyhodnotit lineární závislost či nezávislost vektorů z $\mathbf{R}^n$. Vyšetřované vektory stačí zapsat do řádků matice a spočítat eliminační metodou hodnost této matice (viz algoritmus ??). Je-li hodnost menší, než počet řádků, jsou tyto řádky lineárně závislé. Jinak jsou lineárně nezávislé.

5.34. Příklad. Vektory $(1, 2, 3, 4, 5), (2, 3, 4, 4, 7), (1, 1, 1, 3, 4), (3, 5, 7, 8, 12)$ jsou lineárně závislé, protože odpovídající matice má hodnost 3, jak jsme již spočítali v příkladu ??.

5.35. Algoritmus. Věta ?? společně s definicí hodnosti matice jako dimenzi lineárního obalu řádků matice ?? nám dává návod, jak vyhodnotit, zda dva lineární obaly jsou stejné. Nechť $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ a $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$ jsou vektory z $\mathbf{R}^n$ a cílem je ověřit, zda $\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle = \langle \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m \rangle$, Do řádků matice $\mathbf{A}$ zapíšeme vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$, do řádků matice $\mathbf{B}$ zapíšeme vektory $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$ a konečně do řádků matice $\mathbf{C}$ zapíšeme řádky obou matic společně. Pak uvedené lineární obaly se rovnají, pokud $\operatorname{hod} \mathbf{A} = \operatorname{hod} \mathbf{B} = \operatorname{hod} \mathbf{C}$. Přitom na výpočet hodnosti máme algoritmus ??.

5.36. Příklad. Ověříme, že $\langle (1,2,4,2),(2,5,0,3),(4,9,8,7)\rangle = \langle (1,3,-4,1),(3,7,-4,4)\rangle$.

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 4 & 2 \\ 2 & 5 & 0 & 3 \\ 4 & 9 & 8 & 7 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 4 & 2 \\ 0 & 1 & -8 & -1 \end{pmatrix},$$

$$\mathbf{B} = \begin{pmatrix} 1 & 3 & -4 & 1 \\ 3 & 7 & -4 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & -4 & 1 \\ 0 & 1 & -8 & -1 \end{pmatrix},$$

$$\mathbf{C} = \begin{pmatrix} 1 & 2 & 4 & 2 \\ 2 & 5 & 0 & 3 \\ 4 & 9 & 8 & 7 \\ 1 & 3 & -4 & 1 \\ 3 & 7 & -4 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 4 & 2 \\ 0 & 1 & -8 & -1 \end{pmatrix}$$

Protože $\operatorname{hod}\mathbf{A} = \operatorname{hod}\mathbf{B} = \operatorname{hod}\mathbf{C} = 2$, uvedené lineární obaly se rovnají.

5.37. Algoritmus. Věta ?? společně s definicí hodnosti matice ?? nám dává návod, jak poznat, že nějaký vektor $\boldsymbol{v} \in \mathbf{R}^n$ je prvkem lineárního obalu $\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k\rangle$, kde vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ jsou také prvky z $\mathbf{R}^n$. Stačí do matice $\mathbf{A}$ zapsat po řádcích vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ a do řádků matice $\mathbf{B}$ napsat totéž, ale navíc tam přidat řádek $\boldsymbol{v}$. Pak $\boldsymbol{v}$ leží v uvedeném lineárním obalu, právě když $\operatorname{hod}\mathbf{A} = \operatorname{hod}\mathbf{B}$. Přitom na výpočet hodnosti máme algoritmus ??.

5.38. Příklad. Ověříme, zda $(1,1,12,3) \in \langle (1,2,4,2),(2,5,0,3),(4,9,8,7)\rangle$.

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 4 & 2 \\ 2 & 5 & 0 & 3 \\ 4 & 9 & 8 & 7 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 4 & 2 \\ 0 & 1 & -8 & -1 \end{pmatrix},$$

$$\mathbf{B} = \begin{pmatrix} 1 & 2 & 4 & 2 \\ 2 & 5 & 0 & 3 \\ 4 & 9 & 8 & 7 \\ 1 & 1 & 12 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 4 & 2 \\ 0 & 1 & -8 & -1 \end{pmatrix}.$$

Protože $\operatorname{hod}\mathbf{A} = \operatorname{hod}\mathbf{B} = 2$, leží vektor $(1, 1, 12, 3)$ v uvedeném lineárním obalu.

5.39. Definice. Nechť $\mathbf{A} = (a_{i,j}) \in \mathbf{R}^{m,n}$. Matici $\mathbf{A}^T = (a_{j,i}) \in \mathbf{R}^{n,m}$ nazýváme *transponovanou maticí* k matici $\mathbf{A}$. Matice $\mathbf{A}^T$ tedy vznikne z matice $\mathbf{A}$ přepsáním řádků matice $\mathbf{A}$ do sloupců matice $\mathbf{A}^T$, respektive přepsáním sloupců matice $\mathbf{A}$ do řádků matice $\mathbf{A}^T$.

5.40. Příklad.

$$\text{Je-li třeba } \mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}, \quad \text{pak je } \mathbf{A}^T = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}.$$

5.41. Věta. Pro každou matici $\mathbf{A}$ platí: $(\mathbf{A}^T)^T = \mathbf{A}$.

Důkaz. Věta plyne přímo z definice ??.

5.42. Věta.* Pro každou matici $\mathbf{A} \in \mathbf{R}^{m,n}$ platí: $\operatorname{hod}(\mathbf{A}^T) = \operatorname{hod}(\mathbf{A})$.

Důkaz (pro hloubavé čtenáře). Ukážeme nejprve, že $\operatorname{hod}(\mathbf{A}^T) \geq \operatorname{hod}(\mathbf{A})$. Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$ a označme $k = \operatorname{hod}(\mathbf{A})$. Podle věty ?? existuje k lineárně nezávislých řádků matice $\mathbf{A}$. Označme je $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$. Zapišme si, co to znamená, že tyto řádky jsou lineárně nezávislé. Pro

$$\alpha_1 \boldsymbol{b}_1 + \alpha_2 \boldsymbol{b}_2 + \cdots + \alpha_k \boldsymbol{b}_k = \boldsymbol{o}$$

musí být $\alpha_i = 0\ \forall i \in \{1, \dots, k\}$. Tento požadavek vede na soustavu rovnic, která musí mít jedině triviální řešení:

$$\begin{aligned} \alpha_1\, b_{1,1} + \alpha_2\, b_{2,1} + \cdots + \alpha_k\, b_{k,1} &= 0, \\ \alpha_1\, b_{1,2} + \alpha_2\, b_{2,2} + \cdots + \alpha_k\, b_{k,2} &= 0, \\ &\cdots \\ \alpha_1\, b_{1,n} + \alpha_2\, b_{2,n} + \cdots + \alpha_k\, b_{k,n} &= 0. \end{aligned} \tag{5.1}$$

Koeficienty jednotlivých rovnic soustavy (5.1) odpovídají částem sloupců matice $\mathbf{A}$. Částmi sloupců v tomto důkazu budeme označovat uspořádané k-tice obsahující jen ty prvky z daného sloupce, které leží ve vybraných řádcích $\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_k$. Aby bylo zaručeno pouze triviální řešení soustavy (5.1), musíme po přímém chodu Gaussovy eliminační metody dostat schodovitou matici o k-řádcích (méně řádků by vedlo na nekonečně mnoho řešení). To podle vět ?? a ?? znamená, že existuje k lineárně nezávislých částí sloupců matice $\mathbf{A}$. Tytéž celé sloupce matice $\mathbf{A}$ jsou lineárně nezávislé (kdyby byly závislé, pak by stejná netriviální lineární kombinace celých sloupců dávala nulový vektor i na částech sloupců, ale my víme, že části sloupců jsou lineárně nezávislé). Máme tedy zaručeno, že v matici $\mathbf{A}$ je aspoň k lineárně nezávislých sloupců (zatím není vyloučeno, že jich může být více). Podle věty ?? tedy je $\hod(\mathbf{A}^T) \geq k = \hod(\mathbf{A})$.

Máme $\hod\big((\mathbf{A}^T)^T\big) \geq \hod(\mathbf{A}^T) \geq \hod(\mathbf{A})$, a přitom podle věty ?? je $(\mathbf{A}^T)^T = \mathbf{A}$, takže všechny uvedené hodnosti se rovnají.

5.43. Poznámka. Ukázali jsme, že hodnosti matice $\mathbf{A}$ a $\mathbf{A}^T$ se rovnají. To vysvětluje, proč jsme nedefinovali zvlášť „řádkovou“ hodnost matice jako dimenzi lineárního obalu řádků

a zvlášť „sloupcovou“ hodnost jako dimezi lineárního obalu sloupců. Tato čísla jsou podle věty ?? stejná.

5.44. Věta. Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$. Pak $\mathrm{hod}(\mathbf{A}) \leq \min(m, n)$.

Důkaz. Hodnost matice je menší nebo rovna počtu řádků z věty ?? a je menší nebo rovna počtu sloupců z věty ??.

5.45. Poznámka. Na konci kapitoly ?? jsme uvedli „přílepek“ o spojení a průniku podprostorů. Nyní máme k dispozici větu ??, tedy aparát, pomocí kterého si můžeme tuto problematiku ilustrovat na příkladech.

5.46. Příklad. Jsou dány lineární podprostory M a N lineárního prostoru $\mathbf{R}^5$ pomocí lineárních obalů:

$$M = \big\langle (1,2,0,1,1), (1,3,1,3,4), (3,5,2,4,5) \big\rangle,$$
$$N = \big\langle (1,1,3,4,3), (1,0,2,2,0), (2,1,3,2,3), (0,1,2,4,3) \big\rangle.$$

Najdeme bázi a dimenzi prostorů M, N, $M \cap N$ a $M \vee N$.

Podle věty ?? zachovává Gaussova eliminační metoda lineární obal řádků matice, takže budeme eliminovat následující matice:

$$M\colon\quad \begin{pmatrix} 1 & 2 & 0 & 1 & 1 \\ 1 & 3 & 1 & 3 & 4 \\ 3 & 5 & 2 & 4 & 5 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 \\ 0 & -1 & 2 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 3 & 3 & 5 \end{pmatrix},$$

$$N\colon\quad \begin{pmatrix} 1 & 1 & 3 & 4 & 3 \\ 1 & 0 & 2 & 2 & 0 \\ 2 & 1 & 3 & 2 & 3 \\ 0 & 1 & 2 & 4 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 3 & 4 & 3 \\ 0 & -1 & -1 & -2 & -3 \\ 0 & -1 & -3 & -6 & -3 \\ 0 & 1 & 2 & 4 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 3 & 4 & 3 \\ 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 2 & 4 & 0 \\ 0 & 0 & 1 & 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 3 & 4 & 3 \\ 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 & 0 \end{pmatrix}.$$

Podle věty ?? jsou řádky matic zapsaných nejvíce vpravo lineárně nezávislé. Lineární obal těchto řádků zůstal zachován a je roven M, respektive N. Máme tedy:

$$\begin{aligned} &\text{báze } M\colon && \big\{(1,2,0,1,1),(0,1,1,2,3),(0,0,3,3,5)\big\}, && \dim M = 3,\\ &\text{báze } N\colon && \big\{(1,1,3,4,3),(0,1,1,2,3),(0,0,1,2,0)\big\}, && \dim N = 3. \end{aligned}$$

Vzhledem k tomu, že tři vektory, kterými je zadán podprostor M, jsou lineárně nezávislé, můžeme zapsat i jinou bázi M: $\{(1,2,0,1,1),(1,3,1,3,4),(3,5,2,4,5)\}$. Vektory, kterými je zadán podprostor N jsou lineárně závislé, takže netvoří bázi.

Platí $M \vee N = \langle M \cup N \rangle = \langle \text{báze } M \cup \text{báze } N \rangle$, takže bázi tohoto podprostoru najdeme eliminací následující matice:

$$M \vee N: \quad \begin{pmatrix} 1 & 2 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 3 & 3 & 5 \\ 1 & 1 & 3 & 4 & 3 \\ 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 3 & 3 & 5 \\ 0 & -1 & 3 & 3 & 2 \\ 0 & 0 & 1 & 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 3 & 3 & 5 \\ 0 & 0 & 4 & 5 & 5 \\ 0 & 0 & 1 & 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 3 & 3 & 5 \\ 0 & 0 & 0 & -3 & 5 \\ 0 & 0 & 0 & -3 & 5 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\text{báze } M \vee N: \quad \big\{(1,2,0,1,1), (0,1,1,2,3), (0,0,3,3,5), (0,0,0,-3,5)\big\}, \quad \dim(M \vee N) = 4.$$

Podle věty ?? máme okamžitě dimenzi průniku:

$$\dim(M \cap N) = \dim M + \dim N - \dim(M \vee N) = 3 + 3 - 4 = 2,$$

bohužel nalezení báze průniku dá ještě trochu práce. Vektory společné oběma podprostorům musí jít zapsat jako lineární kombinace báze M i lineární kombinace báze N:

$$\alpha\,(1,2,0,1,1) + \beta\,(0,1,1,2,3) + \gamma\,(0,0,3,3,5) = a\,(1,1,3,4,3) + b\,(0,1,1,2,3) + c\,(0,0,1,2,0). \tag{5.2}$$

Z tohoto požadavku nám vychází soustava pěti rovnic o šesti neznámých $\alpha, \beta, \gamma, a, b, c$. Eliminujeme matici této homogenní soustavy.

$$\begin{pmatrix} 1 & 0 & 0 & -1 & 0 & 0 \\ 2 & 1 & 0 & -1 & -1 & 0 \\ 0 & 1 & 3 & -3 & -1 & -1 \\ 1 & 2 & 3 & -4 & -2 & -2 \\ 1 & 3 & 5 & -3 & -3 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 1 & -1 & 0 \\ 0 & 1 & 3 & -3 & -1 & -1 \\ 0 & 2 & 3 & -3 & -2 & -2 \\ 0 & 3 & 5 & -2 & -3 & 0 \end{pmatrix} \sim \cdots \sim \begin{pmatrix} 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 1 & -1 & 0 \\ 0 & 0 & 3 & -4 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Volíme $b = t$, $c = u$, pak vychází $a = -u$. Ostatní hodnoty proměnných nemusíme počítat a vrátíme se k pravé straně rovnosti (5.2). Vektory, které jsou společné oběma prostorům, musejí tedy splňovat:

$$-u\,(1,1,3,4,3) + t\,(0,1,1,2,3) + u\,(0,0,1,2,0) = t\,(0,1,1,2,3) + u\,(-1,-1,-2,-2,-3).$$

Je tedy $M \cap N = \big\langle (0,1,1,2,3), (1,1,2,2,3) \big\rangle$ a tyto dva vektory tvoří jednu z možných bází lineárního prostoru $M \cap N$. Že průnik obsahuje vektor $(0,1,1,2,3)$ nás nepřekvapí, protože tento vektor byl součástí obou bází podprostorů M i N. Soustavu jsme počítali jen kvůli tomu, abychom našli ten druhý vektor.

5.47. Shrnutí. Množina matic $\mathbf{R}^{m,n}$ tvoří lineární prostor. Vektory z $\mathbf{R}^n$ můžeme ztotožnit s maticemi z $\mathbf{R}^{1,n}$ (řádkové vektory) nebo s maticemi z $\mathbf{R}^{n,1}$ (sloupcové vektory). Řádkové

vektory můžeme klást pod sebe a tvořit matice, nebo můžeme sloupcové vektory klást vedle sebe a rovněž dostáváme matice.

Hodnost matice je dimenze lineárního obalu řádků /??/, což je totéž jako dimenze lineárního obalu sloupců /??/. Na výpočet hodnosti matice se používá algoritmus ??.

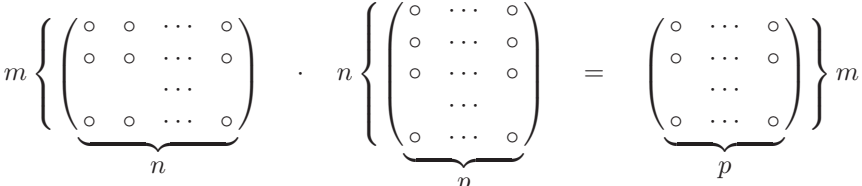
V této kapitole jsme si ukázali algoritmy vycházející z toho, že dané řádkové vektory zapíšeme pod sebe a vytvoříme matici, jejíž hodnost vypočítáme. Algoritmus ?? umožní rozhodnout, zda jsou vektory lineárně závislé či nezávislé. Algoritmus ?? umožní ověřit rovnost obalů a algoritmus ?? odpoví na otázku, zda vektor leží v lineárním obalu daných vektorů.

6. Násobení matic

6.1. Definice.* Nechť $\mathbf{A} = (a_{i,j}) \in \mathbf{R}^{m,n}$ a $\mathbf{B} = (b_{j,k}) \in \mathbf{R}^{n,p}$. Pak je definován *součin matic* $\mathbf{A} \cdot \mathbf{B}$ (v tomto pořadí) jako matice typu (m, p) takto: každý prvek $c_{i,k}$ matice $\mathbf{A} \cdot \mathbf{B}$ je dán vzorcem

$$c_{i,k} = a_{i,1}\, b_{1,k} + a_{i,2}\, b_{2,k} + \cdots + a_{i,n}\, b_{n,k} = \sum_{j=1}^{n} a_{i,j}\, b_{j,k}, \quad i \in \{1, \ldots, m\}, \quad k \in \{1, \ldots, p\}. \tag{6.1}$$

6.2. Poznámka. Všimneme si, že násobení je definováno jen tehdy, pokud počet sloupců první matice je roven počtu řádků druhé matice. Výsledná matice má stejný počet řádků, jako první matice a stejný počet sloupců, jako druhá matice. Názorně:



Každý prvek matice $\mathbf{A} \cdot \mathbf{B}$ přitom musíme počítat podle vzorce (6.1) jako součet součinů odpovídajících prvků řádku první matice a sloupce druhé matice. Začátečníci mohou použít tzv. „dvouprstovou vizuální metodu“: při výpočtu čísla $c_{i,k}$ přiložte ukazováček levé ruky na začátek i-tého řádku první matice a ukazováček pravé ruky na začátek k-tého sloupce druhé matice. Pak pronásobte mezi sebou čísla, na která ukazují prsty, a výsledek uložte do sčítací paměti. Posuňte levý prst na další prvek v řádku a pravý prst na další prvek v sloupci. Znovu vynásobte a přičtěte výsledek ke sčítací paměti. Posunujte dále levý prst v řádku a pravý prst ve sloupci, násobte a sčítejte ve sčítací paměti tak dlouho, dokud nevyčerpáte celý řádek první matice. To se stane podle definice v okamžiku, kdy též vyčerpáte celý sloupec druhé matice. Výsledek sčítací paměti pak napište jako prvek $c_{i,k}$ do postupně budované výsledné matice $\mathbf{A} \cdot \mathbf{B}$.

6.3. Příklad.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 0 & 2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \\ 2 & 7 \end{pmatrix} = \begin{pmatrix} 1\cdot 1+2\cdot 3+3\cdot 5+4\cdot 2 & 1\cdot 2+2\cdot 4+3\cdot 6+4\cdot 7 \\ 5\cdot 1+6\cdot 3+7\cdot 5+8\cdot 2 & 5\cdot 2+6\cdot 4+7\cdot 6+8\cdot 7 \\ 0\cdot 1+2\cdot 3+1\cdot 5+0\cdot 2 & 0\cdot 2+2\cdot 4+1\cdot 6+0\cdot 7 \end{pmatrix} = \begin{pmatrix} 30 \\ 74 \\ 11 \end{pmatrix}$$

6.4. Příklad.*

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ -2 & -2 \end{pmatrix}.$$

Tento příklad ilustruje, že násobení matic obecně nesplňuje komutativní zákon ani pro čtvercové matice, tj. existují matice $\mathbf{A}$, $\mathbf{B}$, pro které neplatí $\mathbf{A} \cdot \mathbf{B} = \mathbf{B} \cdot \mathbf{A}$. Pokud některá z matic $\mathbf{A}$, $\mathbf{B}$ není čtvercová, pak součin $\mathbf{B} \cdot \mathbf{A}$ nemusí být vůbec definován, přestože součin $\mathbf{A} \cdot \mathbf{B}$ definován je.

Příklad dále ukazuje, že není splněna ani vlastnost nuly, na kterou jsme zvyklí při násobení reálných čísel: je-li $a \neq 0$, $b \neq 0$, pak $a\,b \neq 0$. V příkladu násobíme dvě nenulové matice, a přitom dostáváme matici nulovou.

Musíme si z toho odnést ponaučení, že násobení matic nesplňuje všechny vlastnosti, na které jsme zvyklí, a proto při úpravách vzorců obsahujících násobení matic si musíme dát pozor, co můžeme v dané situaci udělat.

Nabízí se přirozená otázka, zda násobení matic splňuje aspoň nějaké zákony, na které jsme zvyklí (jinak by bylo skoro zbytečné tuto operaci nazývat násobením). Následující věta ukazuje, že násobení matic je asociativní a také distributivní vzhledem ke sčítání matic.

6.5. Věta.* Nechť $\alpha \in \mathbf{R}$ a matice $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ jsou odpovídajících typů tak, aby níže uvedené součiny a součty byly definovány. Pak platí

(1) $(\mathbf{A} \cdot \mathbf{B}) \cdot \mathbf{C} = \mathbf{A} \cdot (\mathbf{B} \cdot \mathbf{C})$ (asociativní zákon),

(2) $(\mathbf{A} + \mathbf{B}) \cdot \mathbf{C} = \mathbf{A} \cdot \mathbf{C} + \mathbf{B} \cdot \mathbf{C}$ (distributivní zákon),

(3) $\mathbf{C} \cdot (\mathbf{A} + \mathbf{B}) = \mathbf{C} \cdot \mathbf{A} + \mathbf{C} \cdot \mathbf{B}$ (distributivní zákon),

(4) $\alpha(\mathbf{A} \cdot \mathbf{B}) = (\alpha\, \mathbf{A}) \cdot \mathbf{B} = \mathbf{A} \cdot (\alpha\, \mathbf{B})$,

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

Důkaz. Jako cvičení doplňte ke každému vzorci věty předpoklady o typech matic. Tyto předpoklady se budou pro různé vzorce lišit. V tomto důkazu předpokládáme typy matic (m, n), (n, p) a (p, q).

(1) Označme $\mathbf{A} = (a_{i,j})$, $\mathbf{B} = (b_{j,k})$, $\mathbf{C} = (c_{k,l})$, $\mathbf{A} \cdot \mathbf{B} = (d_{i,k})$, $\mathbf{B} \cdot \mathbf{C} = (f_{j,l})$, $(\mathbf{A} \cdot \mathbf{B}) \cdot \mathbf{C} = (g_{i,l})$, $\mathbf{A} \cdot (\mathbf{B} \cdot \mathbf{C}) = (h_{i,l})$ pro $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, n\}$, $k \in \{1, \ldots, p\}$, $l \in \{1, \ldots, q\}$. Jde o to ukázat, že $g_{i,l} = h_{i,l}$ pro všechna $i \in \{1, \ldots, m\}$ a $l \in \{1, \ldots, q\}$. Podle definice ?? je

$$d_{i,k} = \sum_{j=1}^{n} a_{i,j}\, b_{j,k}, \qquad f_{j,l} = \sum_{k=1}^{p} b_{j,k}\, c_{k,l},$$

takže platí

$$g_{i,l} = \sum_{k=1}^{p} d_{i,k}\, c_{k,l} = \sum_{k=1}^{p} \left(\sum_{j=1}^{n} a_{i,j}\, b_{j,k} \right) c_{k,l} = \sum_{k=1}^{p} \left(\sum_{j=1}^{n} a_{i,j}\, b_{j,k}\, c_{k,l} \right) = X,$$

$$h_{i,l} = \sum_{j=1}^{n} a_{i,j}\, f_{j,l} = \sum_{j=1}^{n} a_{i,j} \left(\sum_{k=1}^{p} b_{j,k}\, c_{k,l} \right) = \sum_{j=1}^{n} \left(\sum_{k=1}^{p} a_{i,j}\, b_{j,k}\, c_{k,l} \right) = Y.$$

Vysvětlíme si, proč platí $X = Y$. Volme i, l pevná. Součiny $a_{i,j} \cdot b_{j,k} \cdot c_{k,l}$ můžeme zapsat do tabulky, ve které index j odpovídá řádku tabulky a index k sloupci. Hodnota X pak znamená součet sloupcových mezisoučtů v tabulce a hodnota Y součet řádkových mezisoučtů. Každá účetní ví, že obě hodnoty musí dát stejný výsledek. My ostatní to snadno nahlédneme.

(2) Označme $\mathbf{A} = (a_{i,j})$, $\mathbf{B} = (b_{i,j})$, $\mathbf{C} = (c_{j,k})$, $(\mathbf{A} + \mathbf{B}) \cdot \mathbf{C} = (d_{i,k})$ pro $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, n\}$, $k \in \{1, \ldots, p\}$. Pak podle definic ?? a ?? platí

$$d_{i,k} = \sum_{j=1}^{n} (a_{i,j} + b_{i,j})\, c_{j,k} = \sum_{j=1}^{n} (a_{i,j}\, c_{j,k} + b_{i,j}\, c_{j,k}) = \sum_{j=1}^{n} a_{i,j}\, c_{j,k} + \sum_{j=1}^{n} b_{i,j}\, c_{j,k},$$

což odpovídá prvkům matice $\mathbf{A} \cdot \mathbf{C} + \mathbf{B} \cdot \mathbf{C}$.

(3) Důkaz bychom provedli obdobně, jako v případě (2).

(4) Označme $\mathbf{A} = (a_{i,j})$, $\mathbf{B} = (b_{j,k})$ pro $i \in \{1, \dots, m\}$, $j \in \{1, \dots, n\}$, $k \in \{1, \dots, p\}$. Platí

$$\alpha \sum_{j=1}^{n} a_{i,j}\, b_{j,k} = \sum_{j=1}^{n} \alpha\, a_{i,j}\, b_{j,k} = \sum_{j=1}^{n} (\alpha\, a_{i,j})\, b_{j,k} = \sum_{j=1}^{n} a_{i,j}\, (\alpha\, b_{j,k}),$$

což dokazuje vzorec: (4).

(5) Označíme $\mathbf{A} = (a_{i,j})$, $\mathbf{B} = (b_{j,k})$, $\mathbf{C} = \mathbf{A} \cdot \mathbf{B} = (c_{i,k})$, $i \in \{1, \dots, m\}$, $j \in \{1, \dots, n\}$, $k \in \{1, \dots, p\}$. Je tedy $\mathbf{A}^T = (\alpha_{j,i})$, $\mathbf{B}^T = (\beta_{k,j})$, kde $\alpha_{j,i} = a_{i,j}$, $\beta_{k,j} = b_{j,k}$. Označme ještě součin $\mathbf{D} = \mathbf{B}^T \cdot \mathbf{A}^T = (d_{k,i})$. Podle definice násobení je

$$c_{i,k} = \sum_{j=1}^{n} a_{i,j}\, b_{j,k} = \sum_{j=1}^{n} \beta_{k,j}\, \alpha_{j,i} = d_{k,i},$$

takže $\mathbf{D}^T = \mathbf{C}$, což dokazuje vzorec (5).

6.6. Příklad. Nechť $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ jsou čtvercové matice. Spočítáme $(\mathbf{A} + \mathbf{B}) \cdot (\mathbf{B} + \mathbf{C})$. Podle (3) ve větě ?? je $(\mathbf{A} + \mathbf{B}) \cdot (\mathbf{B} + \mathbf{C}) = (\mathbf{A} + \mathbf{B}) \cdot \mathbf{B} + (\mathbf{A} + \mathbf{B}) \cdot \mathbf{C} = \mathbf{A} \cdot \mathbf{B} + \mathbf{B} \cdot \mathbf{B} + \mathbf{A} \cdot \mathbf{C} + \mathbf{B} \cdot \mathbf{C}$. Místo zápisu $\mathbf{B} \cdot \mathbf{B}$ budeme užívat zkratku $\mathbf{B}^2$. Konečný výsledek je $\mathbf{A} \cdot \mathbf{B} + \mathbf{B}^2 + \mathbf{A} \cdot \mathbf{C} + \mathbf{B} \cdot \mathbf{C}$.

Jiný příklad: $(\mathbf{A}+\mathbf{B})^2 = (\mathbf{A}+\mathbf{B}) \cdot (\mathbf{A}+\mathbf{B}) = (\mathbf{A}+\mathbf{B}) \cdot \mathbf{A} + (\mathbf{A}+\mathbf{B}) \cdot \mathbf{B} = \mathbf{A}^2 + \mathbf{B}^2 + \mathbf{A} \cdot \mathbf{B} + \mathbf{B} \cdot \mathbf{A}$. Tento výsledek obecně nelze zjednodušit, protože násobení matic není komutativní. Pouze tehdy, když pro tyto matice platí $\mathbf{A} \cdot \mathbf{B} = \mathbf{B} \cdot \mathbf{A}$, můžeme psát výsledek ve tvaru $\mathbf{A}^2 + 2\,\mathbf{A} \cdot \mathbf{B} + \mathbf{B}^2$.

6.7. Poznámka. Matice může vzniknout sestavením menších matic vedle sebe anebo pod sebe. Například:

$$\mathbf{A}_1 = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad \mathbf{A}_2 = \begin{pmatrix} 6 \\ 7 \end{pmatrix}, \quad \mathbf{A}_3 = \begin{pmatrix} 8 & 9 \end{pmatrix}, \quad \mathbf{A}_4 = \begin{pmatrix} 0 \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} \mathbf{A}_1 & \mathbf{A}_2 \\ \mathbf{A}_3 & \mathbf{A}_4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 6 \\ 3 & 4 & 7 \\ 8 & 9 & 0 \end{pmatrix}$$

Zde na matici $\mathbf{B}$ můžeme pohlížet jako na matici sestavenou například z bloků $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$, $\mathbf{A}_4$. Bloky kladené vedle sebe musejí mít samozřejmě stejný počet řádků a bloky kladené pod sebe musejí mít stejný počet sloupců.

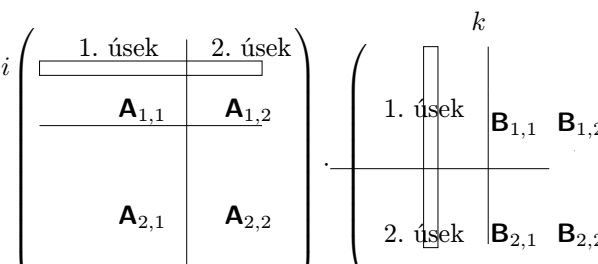
6.8. Věta. Nechť $\mathbf{A}$ a $\mathbf{B}$ jsou matice sestavené po blocích takto:

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_{1,1} & \mathbf{A}_{1,2} \\ \mathbf{A}_{2,1} & \mathbf{A}_{2,2} \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} \mathbf{B}_{1,1} & \mathbf{B}_{1,2} \\ \mathbf{B}_{2,1} & \mathbf{B}_{2,2} \end{pmatrix}$$

Nechť uvedené bloky jsou matice takového typu, že násobení matic $\mathbf{A}_{i,j} \cdot \mathbf{B}_{j,k}$ je definováno pro všechny případy, které se vyskytují v následujícím vzorci. Pak

$$\mathbf{A} \cdot \mathbf{B} = \begin{pmatrix} \mathbf{A}_{1,1} \cdot \mathbf{B}_{1,1} + \mathbf{A}_{1,2} \cdot \mathbf{B}_{2,1} & \mathbf{A}_{1,1} \cdot \mathbf{B}_{1,2} + \mathbf{A}_{1,2} \cdot \mathbf{B}_{2,2} \\ \mathbf{A}_{2,1} \cdot \mathbf{B}_{1,1} + \mathbf{A}_{2,2} \cdot \mathbf{B}_{2,1} & \mathbf{A}_{2,1} \cdot \mathbf{B}_{1,2} + \mathbf{A}_{2,2} \cdot \mathbf{B}_{2,2} \end{pmatrix}$$

Důkaz. Prvek $c_{i,k}$ součinu $\mathbf{A} \cdot \mathbf{B}$ se počítá z prvků i-tého řádku matice $\mathbf{A}$ a k-tého sloupce matice $\mathbf{B}$. Prochází-li i-tý řádek bloky $\mathbf{A}_{1,1}$ a $\mathbf{A}_{1,2}$ a k-tý sloupec bloky $\mathbf{B}_{1,1}$ a $\mathbf{B}_{2,1}$, pak zřejmě součin $\mathbf{A}_{1,1} \cdot \mathbf{B}_{1,1}$ pracuje s prvky prvního úseku i-tého řádku matice $\mathbf{A}$ a prvního úseku k-tého sloupce matice $\mathbf{B}$ a další součin $\mathbf{A}_{1,2} \cdot \mathbf{B}_{2,1}$ bere prvky z druhého úseku i-tého řádku matice $\mathbf{A}$ a druého úseku k-tého sloupce matice $\mathbf{B}$. Prvek $c_{i,k}$ je podle definice maticového součinu ?? součtem odpovídajících prvků na i-tém řádku a k-tém sloupci v maticích $\mathbf{A}_{1,1} \cdot \mathbf{B}_{1,1}$ a $\mathbf{A}_{1,2} \cdot \mathbf{B}_{2,1}$. Analogicky je možno argumentovat v případě, že i-tý řádek nebo k-tý sloupec procházejí jinými bloky. Obtížně se o tom mluví, lepší je si toto maticové násobení „nakreslit“ (viz obrázek).



$$c'_{i,k} = \text{prvek}_{i,k} \text{ matice } \mathbf{A}_{1,1} \cdot \mathbf{B}_{1,1} = (\text{1. úsek } i\text{-tého řádku } \mathbf{A}) \cdot (\text{1. úsek } k\text{-tého sloupce } \mathbf{B})$$
$$c''_{i,k} = \text{prvek}_{i,k} \text{ matice } \mathbf{A}_{1,2} \cdot \mathbf{B}_{2,1} = (\text{2. úsek } i\text{-tého řádku } \mathbf{A}) \cdot (\text{2. úsek } k\text{-tého sloupce } \mathbf{B})$$
$$c_{i,k} = \text{prvek}_{i,k} \text{ matice } \mathbf{A} \cdot \mathbf{B} = (\text{celý } i\text{-tý řádek } \mathbf{A}) \cdot (\text{celý } k\text{-tý sloupec } \mathbf{B}) = c'_{i,k} + c''_{i,k}.$$

6.9. Věta. Nechť $\mathbf{A}$ a $\mathbf{B}$ jsou matice sestavené po blocích takto:

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_{1,1} & \mathbf{A}_{1,2} & \dots & \mathbf{A}_{1,n} \\ \mathbf{A}_{2,1} & \mathbf{A}_{2,2} & \dots & \mathbf{A}_{2,n} \\ & & \dots & \\ \mathbf{A}_{m,1} & \mathbf{A}_{m,2} & \dots & \mathbf{A}_{m,n} \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} \mathbf{B}_{1,1} & \mathbf{B}_{1,2} & \dots & \mathbf{B}_{1,p} \\ \mathbf{B}_{2,1} & \mathbf{B}_{2,2} & \dots & \mathbf{B}_{2,p} \\ & & \dots & \\ \mathbf{B}_{n,1} & \mathbf{B}_{n,2} & \dots & \mathbf{B}_{n,p} \end{pmatrix}$$

Nechť uvedené bloky jsou matice takového typu, že násobení matic $\mathbf{A}_{i,j} \cdot \mathbf{B}_{j,k}$ je definováno pro všechna $i \in \{1, \dots, m\}$, $j \in \{1, \dots, n\}$, $k \in \{1, \dots, p\}$. Tedy počet sloupců bloku $\mathbf{A}_{i,j}$ je roven počtu řádků bloku $\mathbf{B}_{j,k}$. Pak

$$\mathbf{C} = \mathbf{A} \cdot \mathbf{B} = \begin{pmatrix} \mathbf{C}_{1,1} & \mathbf{C}_{1,2} & \dots & \mathbf{C}_{1,p} \\ \mathbf{C}_{2,1} & \mathbf{C}_{2,2} & \dots & \mathbf{C}_{2,p} \\ & & \dots & \\ \mathbf{C}_{m,1} & \mathbf{C}_{m,2} & \dots & \mathbf{C}_{m,p} \end{pmatrix}, \quad \text{kde} \quad \mathbf{C}_{i,k} = \sum_{j=1}^{n} \mathbf{A}_{i,j} \cdot \mathbf{B}_{j,k}.$$

Důkaz. Je zřejmé, že $\mathbf{C}_{i,k}$ je blok typu (u_i, v_k), kde u_i je počet řádků bloku $\mathbf{A}_{i,1}$ a v_k je počet sloupců bloku $\mathbf{B}_{1,k}$ a tento typ mají všechny součiny $\mathbf{A}_{i,j} \cdot \mathbf{B}_{j,k}$ pro všechna $j \in \{1, \dots, n\}$, takže součet součinů ve vzorci pro $\mathbf{C}_{i,k}$ je definován. Větu lze dále dokázat analogicky, jako větu předchozí. Každý řádek matice $\mathbf{A}$ a sloupec matice $\mathbf{B}$ se nyní rozdělí na n úseků.

6.10. Poznámka. Povšimneme si, že pokud volíme ve větě ?? za bloky „matice s jediným číslem“ (matice z $\mathbf{R}^{1,1}$), pak věta rozepisuje definici maticového násobení. Zajímavé jsou pro nás ještě případy, kdy matice $\mathbf{A}$ je rozepsána do řádkových bloků nebo matice $\mathbf{B}$ je rozepsána do sloupcových bloků. To je formulováno v následujících větě.

6.11. Věta. Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$, $\mathbf{B} \in \mathbf{R}^{n,p}$. Nechť matice $\mathbf{B}$ je zapsána po sloupcích: $\mathbf{B} = (\boldsymbol{b}_1\ \boldsymbol{b}_2\ \ldots\ \boldsymbol{b}_p)$, tj. $\boldsymbol{b}_k$ jsou sloupcové vektory z $\mathbf{R}^{n,1}$. Pak

$$\mathbf{A} \cdot \mathbf{B} = (\mathbf{A} \cdot \boldsymbol{b}_1 \quad \mathbf{A} \cdot \boldsymbol{b}_2 \quad \ldots \quad \mathbf{A} \cdot \boldsymbol{b}_p)$$

Důkaz. Stačí v předchozí větě ?? volit matici $\mathbf{A}$ obsahující jediný blok a matici $\mathbf{B}$ obsahující jako bloky své sloupce. V terminologii předchozí věty tedy $m = n = 1$ a $p =$ počet sloupců matice $\mathbf{B}$.

6.12. Poznámka. Věta ?? se dá lapidárně formulovat takto: sloupce maticového součinu $\mathbf{A}\cdot\mathbf{B}$ obsahují součiny celé matice $\mathbf{A}$ s odpovídajícími sloupci matice $\mathbf{B}$. Analogicky lze dokázat, že řádky maticového součinu $\mathbf{A} \cdot \mathbf{B}$ obsahují součiny odpovídajících řádků matice $\mathbf{A}$ s celou maticí $\mathbf{B}$. Tuto větu si přesně zforuluje již laskavý čtenář sám.

6.13. Poznámka. Rozdělme v maticovém součinu $\mathbf{A}\cdot\mathbf{B}$ matici $\mathbf{A}$ na řádky a současně matici $\mathbf{B}$ na sloupce. Pak věta ?? nám říká, že každý prvek součinu $c_{i,k}$ se počítá jako maticový součin i-tého řádku matice $\mathbf{A}$ s k-tým sloupcem matice $\mathbf{B}$. Každý takový součin je roven sumě ve vzorci (6.1). Takže tímto pohledem nezískáme nic jiného, než přímo definici maticového násobení ??.

Jiný pohled na maticový součin dostaneme tím, že matici $\mathbf{A}$ rozdělíme na sloupce a matici $\mathbf{B}$ na řádky. Pak je $\mathbf{A}\cdot\mathbf{B}$ podle věty ?? součtem všech součinů j-tého sloupce matice $\mathbf{A}$ s j-tým řádkem matice $\mathbf{B}$ pro $j \in \{1, 2, \ldots, n\}$. Každý takový součin je tentokrát matice typu (m, p). Maticový součin „sloupec krát řádek“ totiž vytvoří matici typu (m, p), kde m je počet prvků ve sloupci a p je počet prvků v řádku. Na druhé straně maticový součin „řádek krát sloupec“ vytvoří matici typu $(1, 1)$, tedy matici s jediným prvkem.

6.14. Příklad. Jiný pohled na maticový součin z předchozí poznámky ilustrujeme na příkladu ??. Matice vynásobíme tak, že první matici rozdělíme na sloupce a druhou na řádky. Dostáváme

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 0 & 2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \\ 2 & 7 \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \end{pmatrix} + \begin{pmatrix} 2 \\ 6 \\ 2 \end{pmatrix} \cdot \begin{pmatrix} 3 & 4 \end{pmatrix} + \begin{pmatrix} 3 \\ 7 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 5 & 6 \end{pmatrix} + \begin{pmatrix} 4 \\ 8 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 7 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 \\ 5 & 10 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 6 & 8 \\ 18 & 24 \\ 6 & 8 \end{pmatrix} + \begin{pmatrix} 15 & 18 \\ 35 & 42 \\ 5 & 6 \end{pmatrix} + \begin{pmatrix} 8 & 28 \\ 16 & 56 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 30 & 56 \\ 74 & 132 \\ 11 & 14 \end{pmatrix}.$$

6.15. Poznámka. Máme za úkol vynásobit dvě čtvercové matice z $\mathbf{R}^{n,n}$. Jak je to výpočetně náročné? Předpokládejme, že násobení čísel je podstatně „dražší“ operace než sčítání, takže se zaměříme na počet potřebných násobení dvou čísel a počet sčítání budeme zanedbávat.

Pokud budeme postupovat při násobení čvercových matic podle definice ??, budeme potřebovat pro výpočet každého prvku výsledku n operací a těch prvků je n^2, takže dohoromady potřebujeme n^3 operací násobení. Lze na tom někde ušetřit? V následujícím textu ukážeme, že ano, pokud použijeme rekurzivní blokový přístup k násobení matic. Uvedeme nejprve klasickou rekurzi pro násobení a následně tzv. *Strassenův algoritmus*, který rozšiřuje klasickou rekurzi a ušetří operace.

6.16. Algoritmus (klasická rekurze). Předpokládejme, že násobíme čtvercové matice $\mathbf{A}$ a $\mathbf{B}$ z $\mathbf{R}^n$ a že navíc existuje přirozené m tak, že $n = 2^m$. Jinými slovy, každou matici lze rozkájet na čtyři čtvercové bloky stejně velké a tyto bloky lze znovu takto rozkrájet až na úroveň matic typu $(1, 1)$. Jak se zachovat, pokud tento předpoklad není splněn, je zmíněno v poznámce ??.

Proveďme výše zmíněné rozdělení matic $\mathbf{A}$ a $\mathbf{B}$ do bloků a použijme větu ??:

$$\begin{pmatrix} \mathbf{A}_1 & \mathbf{A}_2 \\ \mathbf{A}_3 & \mathbf{A}_4 \end{pmatrix} \cdot \begin{pmatrix} \mathbf{B}_1 & \mathbf{B}_2 \\ \mathbf{B}_3 & \mathbf{B}_4 \end{pmatrix} = \begin{pmatrix} \mathbf{A}_1 \cdot \mathbf{B}_1 + \mathbf{A}_2 \cdot \mathbf{B}_3 & \mathbf{A}_1 \cdot \mathbf{B}_2 + \mathbf{A}_2 \cdot \mathbf{B}_4 \\ \mathbf{A}_3 \cdot \mathbf{B}_1 + \mathbf{A}_4 \cdot \mathbf{B}_3 & \mathbf{A}_3 \cdot \mathbf{B}_2 + \mathbf{A}_4 \cdot \mathbf{B}_4 \end{pmatrix}$$

Vidíme, že algoritmus na násobení matic rekurzivně volá sebe sama celkem osmkrát, ovšem bloky, které se nyní násobí, jsou z $\mathbf{R}^{n/2,n/2}$. Rekurzi můžeme nechat pokračovat až na úrověň bloků z $\mathbf{R}^{1,1}$ a teprve v tom případě násobíme odpovídající čísla mezi sebou.

6.17. Poznámka. Kolik potřebuje klasická rekurze operací násobení čísel? Je-li $F(n)$ počet potřebných operací pro výpočet součinu matic z $\mathbf{R}^{n,n}$, kde $n = 2^m$, pak platí:

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

Potřebujeme tedy stejný počet operací, jako kdybychom použili definici.

6.18. Algoritmus (Strassen). Nechť dvě čtvercové matice $\mathbf{A}$ a $\mathbf{B}$ z $\mathbf{R}^{n,n}$ splňují stejné předpoklady, jako v předchozím algoritmu, tj. $n = 2^m$ a rozdělme matice $\mathbf{A}$, $\mathbf{B}$ do bloků, jako před chvílí. Vypočteme pomocné matice:

$$\mathbf{X}_1 = (\mathbf{A}_1 + \mathbf{A}_4) \cdot (\mathbf{B}_1 + \mathbf{B}_4), \quad \mathbf{X}_2 = (\mathbf{A}_3 + \mathbf{A}_4) \cdot \mathbf{B}_1, \quad \mathbf{X}_3 = \mathbf{A}_1 \cdot (\mathbf{B}_2 - \mathbf{B}_4), \quad \mathbf{X}_4 = \mathbf{A}_4 \cdot (\mathbf{B}_3 -$$
$$\mathbf{X}_5 = (\mathbf{A}_1 + \mathbf{A}_2) \cdot \mathbf{B}_4, \quad \mathbf{X}_6 = (\mathbf{A}_3 - \mathbf{A}_1) \cdot (\mathbf{B}_1 + \mathbf{B}_2), \quad \mathbf{X}_7 = (\mathbf{A}_2 - \mathbf{A}_4) \cdot (\mathbf{B}_3 + \mathbf{B}_4)$$

Čtenář si jako cvičení ověří, že platí:

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

Povšimneme si, že nyní jsme potřebovali pouze sedm maticových násobení, takže voláme rekurzivně sebe sama jen sedmkrát.

6.19. Poznámka. Kolik potřebujeme ve Strassenově algoritmu operací násobení jednotlivých čísel? Předpokládejme matice z $\mathbf{R}^{n,n}$ a $n = 2^m$, neboli $m = \log_2 n$. Nechť $F(n)$ je počet operací násobení použitých ve Strassenově algoritmu, který sestavuje součin matic z $\mathbf{R}^{n,n}$. Pak

$$\begin{aligned} F(n) &= 7F(n/2) = 7(7F(n/4)) = 7(7(7F(n/2^3))) = \cdots = 7^m F(n/2^m) = 7^m F(1) = \\ &= 7^m = (2^{\log_2 7})^{\log_2 n} = 2^{\log_2 7 \cdot \log_2 n} = n^{\log_2 7} \doteq n^{2,807}. \end{aligned}$$

Číslo $n^{2,807}$ je jistě menší než n^3, takže Strassenův algoritmus šetří počet násobení. Pro velká n je úspora natolik výrazná, že přestane být nevýhodou, že potřebujeme poněkud více sčítání. V knihovnách pro násobení velkých matic se proto typicky používá Strassenův algoritmus.

6.20. Poznámka. V článku [7] Don Coppersmith a Shmuel Winograd uvádějí algoritmus, který má ještě lepší složitost: $n^{2,376}$, ovšem přidává tolik dodatečných režijních operací a

paměťových nároků, že by byl užitečný jen pro tak rozsáhlé matice, které se v současné době nevejdou do počítače. Používá se tedy jen jako teoretická dosud známá nejlepší mez složitosti pro maticové násobení. Dosud přitom není dokázáno, jaká je skutečná nejlepší mez, tj. zda by bylo možné toto číslo ještě vylepšit.

6.21. Poznámka. Pokud násobíme matice, které nejsou čvercové nebo nejsou typu $(2^m, 2^m)$, pak je potřeba rozšířit matice o nulové řádky nebo sloupce nebo obojí tak, aby rozšířené matice byly typu $(2^m, 2^m)$. Pak je možné použít výše uvedené rekurzivní algoritmy. V nich můžeme hlídat rozsah indexů jednotlivých bloků a pokud je celý blok v prostoru, kde jsou jen nuly, nemusí algoritmus součin počítat a rovnou vrátí jako výsledek nulový blok. Je to pouze technická vychytávka výše popsaných algoritmů, která neovlivní teoretické výsledky, o kterých jsme se zmínili dříve. Ve výsledku je pak potřeba zpětně odebrat rozšiřující řádky a sloupce (které stejně vyjdou nulové).

6.22. Definice. Nechť je dána čtvercová matice $\mathbf{A} \in \mathbf{R}^{n,n}$. Pokud matice $\mathbf{B}$ splňuje rovnost $\mathbf{A} \cdot \mathbf{B} = \mathbf{B} \cdot \mathbf{A}$, říkáme, že matice $\mathbf{B}$ *komutuje* s maticí $\mathbf{A}$.

6.23. Příklad. Zabývejme se vlastnostmi matic $\mathbf{B}$, které komutují s pevně danou čtvercovou maticí $\mathbf{A} \in \mathbf{R}^{n,n}$. Například matice $\mathbf{A}$ komutuje sama se sebou, neboť součin $\mathbf{A} \cdot \mathbf{A}$ je pro čtvercovou matici definován a prohození činitelů vůbec nepoznáme.

Matice $\mathbf{B}$ komutující s $\mathbf{A}$ musí mít stejný počet řádků jako matice $\mathbf{A}$ sloupců (aby bylo definováno $\mathbf{A}\cdot\mathbf{B}$) a také musí mít stejný počet sloupců jako matice $\mathbf{A}$ řádků (aby bylo definováno $\mathbf{B}\cdot\mathbf{A}$). To prakticky znamená, že matice $\mathbf{B}$ musí být také čtvercová, typu (n,n).

Z příkladu ?? víme, že ne všechny matice z $\mathbf{R}^{n,n}$ komutují s danou čtvercovou maticí. Takže množina čtvercových matic komutujících s danou maticí $\mathbf{A}$ bude tvořit pomnožinu všech čtvercových matic. Ukážeme, že tato podmnožina je lineárním podprostorem všech čtvercových matic.

Podle definice ?? stačí ukázat, že pokud jsou $\mathbf{B}$ a $\mathbf{C}$ komutující matice s maticí $\mathbf{A}$ a $\alpha\in\mathbf{R}$, pak též $\mathbf{B}+\mathbf{C}$ a $\alpha\,\mathbf{B}$ jsou komutující matice. Předpokládejme tedy, že platí $\mathbf{A}\cdot\mathbf{B}=\mathbf{B}\cdot\mathbf{A}$, $\mathbf{A}\cdot\mathbf{C}=\mathbf{C}\cdot\mathbf{A}$. V následujícím výpočtu použijeme věty ??, vzorce (2) až (4) a našeho předpokladu.

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

6.24. Příklad. Najdeme bázi a dimenzi lineárního podprostoru M všech matic komutujících s maticí

$$\mathbf{A}=\begin{pmatrix}1&2\\3&4\end{pmatrix}.$$

Podle předchozího příkladu musejí být matice komutující s maticí $\mathbf{A}$ rovněž typu $(2,2)$. Předpokládejme, že matice $\mathbf{B}$ lze zapsat ve tvaru

$$\mathbf{B} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Jednotlivé součiny pak vypadají následovně

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} a+3b & 2a+4b \\ c+3d & 2c+4d \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+2c & b+2d \\ 3a+4c & 3b+4d \end{pmatrix}.$$

Tyto součiny se mají rovnat. Podle poznámky ?? se dvě matice rovnají, pokud se vzájemně rovnají všechny jejich odpovídající prvky. To nás vede ke čtyřem rovnicím o čtyřech neznámých, které upravíme Gaussovou elmininační metodou.

$$\begin{array}{rrrrl} & 3b & -2c & = 0 \\ 2a & +3b & & -2d = 0 \\ -3a & & -3c & +3d = 0 \\ & -3b & +2c & = 0 \end{array} \quad \begin{pmatrix} 0 & 3 & -2 & 0 \\ 2 & 3 & 0 & -2 \\ -1 & 0 & -1 & 1 \\ 0 & -3 & 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 0 & -2 \\ 0 & 3 & -2 & 0 \end{pmatrix} \quad \begin{array}{rrrl} 2a & +3b & & -2d \\ & 3b & -2c & \end{array}$$

Proměnné c a d můžeme volit libovolně. Uvedené dvě rovnice nám umožňují dopočítat proměnné b a a takto: $b = 2/3\,c$, $a = d - c$. Všechny matice, které komutují s maticí $\mathbf{A}$ jsou tedy

určeny dvěma parametry:

$$\mathbf{B} = \begin{pmatrix} d-c & \frac{2}{3}c \\ c & d \end{pmatrix} = c\begin{pmatrix} -1 & \frac{2}{3} \\ 1 & 0 \end{pmatrix} + d\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad c \in \mathbf{R}, \quad d \in \mathbf{R}.$$

Lineární prostor všech komutujících matic M se nám podařilo vyjádřit jako množinu všech lineárních kombinací dvou konstantních matic. Tuto skutečnost zapíšeme pomocí lineárního obalu takto:

$$M = \left\langle \begin{pmatrix} -1 & \frac{2}{3} \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} -3 & 2 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle.$$

Poslední úpravu (pronásobení první matice třemi) jsme nemuseli dělat, pokud se spokojíme se zlomkem ve výsledku. V modelových příkladech se dosti často snažíme dostat výsledek vyjádřitelný v malých celých číslech. Není to samozřejmě naší povinností, pouze pak výsledek lépe vypadá a nás více potěší.

Protože poslední dvě uvedené matice jsou lineárně nezávislé (to snadno zjistíme) a jejich lineární obal je celý podprostor M, máme výsledek:

$$\text{Báze } M = \left\{ \begin{pmatrix} -3 & 2 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}, \quad \text{tj. } \dim M = 2.$$

6.25. Poznámka. V definici ?? jsme zavedli matice, jejíž prvky jsou reálná nebo komplexní čísla. Občas se můžeme setkat s maticemi, jejíž prvky jsou vektory, tedy prvky libovolného lineárního prostoru. Protože lze prvky lineárního prostoru podle definice ?? násobit reálným číslem, lze přirozeně definovat též maticové násobení $\mathbf{A} \cdot \mathbf{B}$, kde $\mathbf{A} = (a_{i,j}) \in \mathbf{R}^{m,n}$ je matice reálných čísel a $\mathbf{B} = (\boldsymbol{b}_{j,k})$ je matice typu (n, p) obsahující vektory lineárního prostoru L, tedy $\mathbf{B} \in L^{n,p}$. Výsledná matice $\mathbf{A} \cdot \mathbf{B}$ je z množiny $L^{m,p}$ a pro její prvky $\boldsymbol{c}_{i,k}$ platí:

$$\boldsymbol{c}_{i,k} = a_{i,1}\,\boldsymbol{b}_{1,k} + a_{i,2}\,\boldsymbol{b}_{2,k} + \cdots + a_{i,n}\,\boldsymbol{b}_{n,k} = \sum_{j=1}^{n} a_{i,j}\,\boldsymbol{b}_{j,k}.$$

6.26. Příklad. Nechť $\mathbf{A} \in \mathbf{R}^{1,n}$ je matice reálných čísel a $\mathbf{B} \in L^{n,1}$ Pak součin $\mathbf{A} \cdot \mathbf{B}$ je lineární kombinace vektorů z $\mathbf{B}$, přičemž prvky z $\mathbf{A}$ jsou koeficienty této lineární kombinace. Názorně:

$$(\,a_1,\quad a_2,\quad \cdots,\quad a_n\,) \cdot \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \\ \vdots \\ \boldsymbol{b}_n \end{pmatrix} = a_1\,\boldsymbol{b}_1 + a_2\,\boldsymbol{b}_2 + \cdots + a_n\,\boldsymbol{b}_n.$$

6.27. Poznámka.* Předchozí příklad nám poskytuje další pohled na maticové násobení. Předpokládejme matice $\mathbf{A} \in \mathbf{R}^{m,n}$, $\mathbf{B} \in \mathbf{R}^{n,p}$, $\mathbf{C} = \mathbf{A} \cdot \mathbf{B} \in \mathbf{R}^{m,p}$. Na matici $\mathbf{B}$ se dívejme jako

na jednosloupcovou matici jejích řádků. První řádek výsledné matice $\mathbf{C}$ obsahuje lineární kombinaci řádků matice $\mathbf{B}$, přičemž koeficienty této lineární kombince jsou v prvním řádku matice $\mathbf{A}$. Také každý k-tý řádek matice $\mathbf{C}$ obsahuje lineární kombinaci všech řádků matice $\mathbf{B}$ a její koeficienty jsou v k-tém řádku matice $\mathbf{A}$.

6.28. Věta.* Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$, $\mathbf{B} \in \mathbf{R}^{n,p}$. Pak $\hod(\mathbf{A} \cdot \mathbf{B}) \leq \hod \mathbf{A}$ a také $\hod(\mathbf{A} \cdot \mathbf{B}) \leq \hod \mathbf{B}$. Jinými slovy: hodnost maticového součinu není větší než hodnosti jednotlivých činitelů.

Důkaz. Podle poznámky ?? víme, že řádky matice $\mathbf{AB}$ jsou lineárními kombinacemi řádků matice $\mathbf{B}$. Takže $\mathrm{r}\colon \mathbf{AB} \subseteq \langle \mathrm{r}\colon \mathbf{B} \rangle$, tj. $\langle \mathrm{r}\colon \mathbf{AB} \rangle \subseteq \langle \langle \mathrm{r}\colon \mathbf{B} \rangle \rangle = \langle \mathrm{r}\colon \mathbf{B} \rangle$. Podle věty ?? tedy je $\dim \langle \mathrm{r}\colon \mathbf{AB} \rangle \leq \dim \langle \mathrm{r}\colon \mathbf{B} \rangle$, neboli $\hod(\mathbf{A} \cdot \mathbf{B}) \leq \hod \mathbf{B}$.

Protože platí věty ?? a ??, můžeme psát $\hod(\mathbf{A} \cdot \mathbf{B}) = \hod(\mathbf{A} \cdot \mathbf{B})^T = \hod(\mathbf{B}^T \cdot \mathbf{A}^T)$ a z právě dokázané nerovnosti plyne, že $\hod(\mathbf{B}^T \cdot \mathbf{A}^T) \leq \hod \mathbf{A}^T = \hod \mathbf{A}$. Dokázali jsme $\hod(\mathbf{A} \cdot \mathbf{B}) \leq \hod \mathbf{A}$.

6.29. Definice. Čtvercovou matici $\mathbf{E} \in \mathbf{R}^{n,n}$ nazýváme *jednotkovou maticí*, pokud pro její prvky $e_{i,j}$ platí: $e_{i,j} = 0$ pro $i \neq j$ a $e_{i,j} = 1$ pro $i = j$. Názorně:

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

6.30. Poznámka. Z definice maticového násobení okamžitě plyne, že pro každou čtvercovou matici $\mathbf{A} \in \mathbf{R}^{n,n}$ je $\mathbf{E} \cdot \mathbf{A} = \mathbf{A} \cdot \mathbf{E} = \mathbf{A}$. Jednotková matice má tedy stejnou vlastnost vzhledem k násobení, jako jednička při násobení reálných čísel. Pro reálná čísla taky platí, že $1 \cdot a = a \cdot 1 = a$.

Všimneme si také, že jednotková matice je komutující s každou čtvercovou maticí.

6.31. Poznámka. Vraťme se k příkladu ??. Tam jsme našli bázi, ve které je jednotková matice. To nás nepřekvapí, protože jednotková matice je komutující s každou maticí. Dále s maticí $\mathbf{A}$ komutuje stejná matice $\mathbf{A}$. Pokud víme, že $\dim M = 2$ a matice $\mathbf{A}$ a $\mathbf{E}$ jsou lineárně nezávislé, můžeme rovnou prohlásit, že hledaná báze lineárního podprostoru M je $\{\mathbf{A}, \mathbf{E}\}$. Zdálo by se, že jsme výpočty v příkladu ?? dělali zbytečně. Není to tak docela pravda, protože dopředu nevíme, zda dimenze hledaného prostoru bude rovna dvěma.

6.32. Poznámka. V definici ?? jsme zavedli jednotkovou matici s podobnými vlastnostmi, jako má reálné číslo 1. Vraťme se znovu ke srovnání s reálnými čísly. Pro každé nenulové reálné číslo a existuje reálné číslo b takové, že $ab = 1$. Takové reálné číslo obvykle nazýváme převrácenou hodnotou čísla a a označujeme $1/a$ nebo též a^{-1}. Analogicky definujeme „převrácenou hodnotu matice“, tzv. inverzní matici.

6.33. Definice.* Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$ je čtvercová matice a $\mathbf{E} \in \mathbf{R}^{n,n}$ je jednotková matice. Matici $\mathbf{B} \in \mathbf{R}^{n,n}$, která splňuje vlastnost $\mathbf{A} \cdot \mathbf{B} = \mathbf{E} = \mathbf{B} \cdot \mathbf{A}$ nazýváme *inverzní maticí* k matici $\mathbf{A}$. Inverzní matici k matici $\mathbf{A}$ označujeme symbolem $\mathbf{A}^{-1}$.

6.34. Věta. Pokud k matici $\mathbf{A}$ existuje inverzní matice, pak je tato inverzní matice jednoznačně určena.

Důkaz. Nechť má čtvercová matice $\mathbf{A}$ dvě inverzní matice $\mathbf{B}$ a $\mathbf{C}$. Ukážeme, že pak $\mathbf{B} = \mathbf{C}$. Platí:

$$\mathbf{B} = \mathbf{B} \cdot \mathbf{E} = \mathbf{B} \cdot (\mathbf{A} \cdot \mathbf{C}) = (\mathbf{B} \cdot \mathbf{A}) \cdot \mathbf{C} = \mathbf{E} \cdot \mathbf{C} = \mathbf{C}. \tag{6.2}$$

Zde jsme po řadě využili: poznámku ??, vlastnost, že $\mathbf{C}$ je inverzní matice k $\mathbf{A}$, vlastnost (1) z věty ??, vlastnost, že $\mathbf{B}$ je inverzní matice k $\mathbf{A}$, a konečně znovu poznámku ??.

6.35. Definice.* Čtvercová matice $\mathbf{A} \in \mathbf{R}^{n,n}$ se nazývá *regulární*, pokud pro $\mathbf{A}$ existuje inverzní matice. Čtvercová matice $\mathbf{A} \in \mathbf{R}^{n,n}$ se nazývá *singulární*, pokud není regulární.

6.36. Věta. Matice $\mathbf{A}$ je regulární právě když $\operatorname{hod} \mathbf{A} = n$, kde n je počet řádků matice $\mathbf{A}$.

Důkaz. Nechť $\mathbf{A}$ je regulární, takže existuje $\mathbf{A}^{-1}$ tak, že $\mathbf{A} \cdot \mathbf{A}^{-1} = \mathbf{E}$. Podle věty ?? se hodnost matice součinem nezvětší. Tedy $\operatorname{hod} \mathbf{E} = \operatorname{hod}(\mathbf{A} \cdot \mathbf{A}^{-1}) \leq \operatorname{hod} \mathbf{A}$. Zjevně je $\operatorname{hod} \mathbf{E} = n$, takže musí $\operatorname{hod} \mathbf{A} = n$.

Nechť $\operatorname{hod} \mathbf{A} = n$. Takže řádky matice $\mathbf{A}$ jsou lineárně nezávislé a tvoří bázi $\mathbf{R}^n$. Označme ji (B). Souřadnice i-tého řádku matice $\mathbf{E}$ vzhledem k (B) napišme do i-tého řádku matice $\mathbf{B}$. Zřejmě je $\mathbf{B} \cdot \mathbf{A} = \mathbf{E}$ (viz poznamku ??). Protože $\operatorname{hod} \mathbf{A} = \operatorname{hod} \mathbf{A}^T$, jsou i sloupce matice $\mathbf{A}$

lineárně nezávislé a tvoří bázi (B') lineárního prostoru $\mathbf{R}^n$. Souřadnice i-tého sloupce matice $\mathbf{E}$ vzhledem k (B') napišme do i-tého sloupce matice $\mathbf{C}$. Zřejmě je $\mathbf{C}^T \cdot \mathbf{A}^T = \mathbf{E}$, neboli $\mathbf{A} \cdot \mathbf{C} = \mathbf{E}^T = \mathbf{E}$. Z rovností $\mathbf{B} \cdot \mathbf{A} = \mathbf{E}$ a $\mathbf{A} \cdot \mathbf{C} = \mathbf{E}$ plyne $\mathbf{B} = \mathbf{C}$. Proč? Stačí zopakovat výpočet (6.2), který jsme provedli v důkazu věty ??. Podle definice je $\mathbf{B}$ inverzní matice k matici $\mathbf{A}$. Matice $\mathbf{A}$ je tedy regulární.

6.37. Věta. Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$. Z existence matice $\mathbf{B}$ takové, že $\mathbf{B} \cdot \mathbf{A} = \mathbf{E}$, plyne, že $\mathbf{A}$ je regulární a $\mathbf{B}$ je její inverzní matice. Z existence matice $\mathbf{C}$ takové, že $\mathbf{A} \cdot \mathbf{C} = \mathbf{E}$, plyne, že $\mathbf{A}$ je regulární a $\mathbf{C}$ je její inverzní matice.

Důkaz. Stačí trasovat důkaz předchozí věty. Z existence $\mathbf{B}$ a z věty ?? plyne, že $n = \hod(\mathbf{B} \cdot \mathbf{A}) \leq \hod \mathbf{A}$, takže $\hod \mathbf{A} = n$. Nyní sestavíme matici $\mathbf{C}$ jako v předchozím důkazu a ukážeme, že $\mathbf{A} \cdot \mathbf{C} = \mathbf{E}$ a navíc $\mathbf{B} = \mathbf{C}$, takže je to inverzní matice k matici $\mathbf{A}$. Vyjdeme-li z existence matice $\mathbf{C}$, postupujeme obdobně.

6.38. Poznámka. Předchozí věta říká, že v definici ?? je jedna z rovností $\mathbf{A} \cdot \mathbf{B} = \mathbf{E}$, $\mathbf{B} \cdot \mathbf{A} = \mathbf{E}$ „nadbytečná“, protože z jedné rovnice plyne druhá a z druhé plyne první.

6.39. Věta. Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$ a $\mathbf{B} \in \mathbf{R}^{n,n}$ jsou regulární čtvercové matice. Pak matice $\mathbf{A} \cdot \mathbf{B}$ je rovněž regulární matice typu (n, n).

Důkaz. Matice $\mathbf{A} \cdot \mathbf{B}$ je čtvercová typu (n, n). To plyne přímo z definice maticového součinu. Stačí tedy dokázat, že je regulární. Podle definice ?? je matice regulární právě tehdy, když k ní existuje inverzní matice. Podle předpokladu k matici $\mathbf{A}$ existuje inverzní matice $\mathbf{A}^{-1}$ a k matici $\mathbf{B}$ existuje inverzní matice $\mathbf{B}^{-1}$. Stačí ukázat, že existuje inverzní matice k matici $\mathbf{A} \cdot \mathbf{B}$. Hledaná inverzní matice je tvaru $\mathbf{B}^{-1} \cdot \mathbf{A}^{-1}$, protože:

$$(\mathbf{B}^{-1} \cdot \mathbf{A}^{-1}) \cdot (\mathbf{A} \cdot \mathbf{B}) = \mathbf{B}^{-1} \cdot (\mathbf{A}^{-1} \cdot \mathbf{A}) \cdot \mathbf{B} = \mathbf{B}^{-1} \cdot \mathbf{E} \cdot \mathbf{B} = \mathbf{B}^{-1} \cdot \mathbf{B} = \mathbf{E}.$$

6.40. Příklad.* Na jednoduchém příkladu ukážeme obvyklý postup hledání inverzní matice k dané matici $\mathbf{A}$. Teprve pak dokážeme, že tento postup je oprávněný a vždy vede k inverzní matici.

Naším úkolem bude najít inverzní matici k matici

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ -1 & 0 & 1 \\ 2 & 2 & 1 \end{pmatrix}.$$

Vedle prvků matice $\mathbf{A}$ napíšeme prvky jednotkové matice stejného typu (oddělíme od sebe pro přehlednost svislou čarou) a dále použijeme řádkové úpravy Gaussovy eliminační metody na matici $(\mathbf{A}|\mathbf{E})$ jako celek. To znamená, že pracujeme s řádky délky $2n$, v našem konkrétním

případě s řádky o šesti prvcích. Při eliminaci se snažíme vlevo od svislé čáry dostat postupně jednotkovou matici.

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

$$\sim \left(\begin{array}{ccc|ccc} 1 & 2 & 0 & -2 & 3 & 3 \\ 0 & 2 & 0 & -3 & 5 & 4 \\ 0 & 0 & 1 & 1 & -1 & -1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -2 & -1 \\ 0 & 1 & 0 & -\frac{3}{2} & \frac{5}{2} & 2 \\ 0 & 0 & 1 & 1 & -1 & -1 \end{array}\right), \quad \mathbf{A}^{-1} = \left(\begin{array}{ccc} 1 & -2 & - \\ -\frac{3}{2} & \frac{5}{2} & \\ 1 & -1 & - \end{array}\right)$$

Při přechodu z matice **A** na matici **E** v levém bloku jsme nejprve převedli matici **A** na schodovitou matici stejně, jako je popsáno v úvodní kapitole o Gaussově eliminační metodě (tzv. *přímý chod eliminační metody*). Jsou-li ve schodovité matici na diagonále nenulové prvky, lze pokračovat tzv. *zpětným chodem eliminační metody*. V něm nejprve násobíme poslední řádek vhodnými konstantami a přičítáme k řádkům nad ním. Tím dostáváme nuly v posledním sloupci nad nenulovým prvkem na pozici (n, n). Pak přičítáme násobky předposledního řádku k předchozím a získáme nuly v předposledním sloupci. Takto postupně pokračujeme až dostaneme matici s nenulovými prvky na diagonále a s nulovými prvky jinde. Každý řádek takové matice vynásobíme převrácenou hodnotou jeho diagonálního prvku a dostáváme matici **E**.

Tvrdíme, že hledaná inverzní matice k matici **A** je zapsána vpravo od svislé čáry v poslední úpravě. Zformulujeme to jako algoritmus:

6.41. Algoritmus.* Pokud $(\mathbf{A}\,|\,\mathbf{E}) \sim (\mathbf{E}\,|\,\mathbf{B})$, kde „$\sim$“ znamená konečně mnoho řádkových úprav matice podle Gaussovy eliminační metody, pak $\mathbf{B} = \mathbf{A}^{-1}$.

Zvídavý čtenář se oprávněně ptá, proč tato metoda dává inverzní matici. Sformulujeme tuto vlastnost jako větu ??. Nejprve si ale povšimneme důležité vlastnosti Gaussovy eliminace.

6.42. Věta.* Nechť $\mathbf{A} \sim \mathbf{B}$ jsou dvě matice. Pak existuje matice $\mathbf{P}$ taková, že $\mathbf{B} = \mathbf{P} \cdot \mathbf{A}$.

Důkaz. Protože podle věty ?? je $\langle \mathrm{r}\colon \mathbf{A}\rangle = \langle \mathrm{r}\colon \mathbf{B}\rangle$, jsou řádky matice $\mathbf{B}$ lineárními kombinacemi řádků matice $\mathbf{A}$. Zapíšeme-li koeficienty těchto lineárních kombinací do řádků matice $\mathbf{P}$, dostáváme podle poznámky ?? vztah $\mathbf{P} \cdot \mathbf{A} = \mathbf{B}$.

6.43. Věta. Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$ a nechť lze provést $(\mathbf{A}\,|\,\mathbf{E}) \sim (\mathbf{E}\,|\,\mathbf{B})$, kde „$\sim$“ označuje konečný počet řádkových úprav podle eliminační metody a $\mathbf{E}$ značí jednotkovou matici z $\mathbf{R}^{n,n}$. Pak $\mathbf{B} = \mathbf{A}^{-1}$.

Důkaz. Podle věty ?? existuje matice $\mathbf{P}$ taková, že

$$(\mathbf{A}\,|\,\mathbf{E}) \sim (\mathbf{E}\,|\,\mathbf{B}) = \mathbf{P} \cdot (\mathbf{A}\,|\,\mathbf{E}) = (\mathbf{PA}\,|\,\mathbf{PE}).$$

Protože $\mathbf{B} = \mathbf{PE}$, je $\mathbf{P} = \mathbf{B}$. Protože $\mathbf{E} = \mathbf{PA}$, je $\mathbf{E} = \mathbf{BA}$. Podle věty ?? je $\mathbf{B}$ inverzní matice k matici $\mathbf{A}$.

6.44. Poznámka. Kdybychom napsali jednotkovou matici pod matici $\mathbf{A}$ a aplikovali na sloupce této „dvojmatice“ sloupcové úpravy podle Gaussovy eliminační metody a získali nakonec v horní části matici $\mathbf{E}$, pak je ve spodní části matice inverzní. Při důkazu tohoto tvrzení bychom postupovali analogicky jako při řádkové metodě, jen maticemi $\mathbf{P}_i$, které „emulují“ sloupcové úpravy, bychom násobili matici $\mathbf{A}$ zprava a nikoli zleva.

Rozmyslete si, že není možné při metodě hledání inverzní matice kombinovat řádkové i sloupcové operace dohromady. Naráží to na skutečnost, že násobení matic není komutativní.

6.45. Věta.* Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$ je čtvercová matice. Pak následující podmínky jsou ekvivalentní:
(1) $\mathbf{A}$ je regulární,
(2) $\mathbf{A}$ má inverzní matici $\mathbf{A}^{-1}$,
(3) $\hod \mathbf{A} = n$,
(4) Maticová rovnice $\mathbf{AX} = \mathbf{B}$ s neznámou maticí $\mathbf{X} \in \mathbf{R}^{n,m}$ má řešení pro každou $\mathbf{B} \in \mathbf{R}^{n,m}$.
(5) $\mathbf{A} \sim \mathbf{E}$, tj. existuje konečně kroků Gaussovy eliminační metody, které převedou $\mathbf{A}$ na $\mathbf{E}$.

Důkaz. (1) $\Leftrightarrow$ (2) přímo z definice regulární matice. (2) $\Leftrightarrow$ (3) z věty ??.

Ekvivalence zbývajících podmínek vyplyne z implikací (2) $\Rightarrow$ (4) $\Rightarrow$ (3) $\Rightarrow$ (5) $\Rightarrow$ (2).

(2) $\Rightarrow$ (4): protože $\mathbf{A}^{-1}\mathbf{B}$ uvedenou rovnici řeší. Skutečně je $\mathbf{A}(\mathbf{A}^{-1}\mathbf{B}) = (\mathbf{A}\mathbf{A}^{-1})\mathbf{B} = \mathbf{E}\mathbf{B} = \mathbf{B}$.

(4) $\Rightarrow$ (3): Je-li $\mathbf{C}$ řešení rovnice $\mathbf{AX} = \mathbf{E}$, pak musí podle věty ?? být $\hod \mathbf{E} = \hod(\mathbf{A}\cdot\mathbf{C}) \leq \hod \mathbf{A}$. Protože $\hod \mathbf{E} = n$, musí $\hod \mathbf{A} = n$.

(3) $\Rightarrow$ (5): Protože eliminace nemění hodnost, musí se po přímém chodu Gaussovy eliminace matice $\mathbf{A}$ proměnit ve schodovitou matici s nenulovými řádky, tedy s nenulovými čísly na diagonále. Pak lze provést zpětný chod eliminace a převést původní matici $\mathbf{A}$ na $\mathbf{E}$.

(5) $\Rightarrow$ (2): Je-li $\mathbf{A} \sim \mathbf{E}$, pak $(\mathbf{A} \,|\, \mathbf{E}) \sim (\mathbf{E} \,|\, \mathbf{A}^{-1})$ podle věty ??.

6.46. Poznámka. Další ekvivalentní podmínkou regularity matice $\mathbf{A}$ je lineární nezávislost jejích řádků (podle věty ??) což je ekvivalentní s lineární nezávislosti sloupců (podle věty ??) a to je ekvivalentní s regularitou matice $\mathbf{A}^T$. V následující kapitole si ještě ukážeme, že $\mathbf{A}$ je regulární právě tehdy, když má nenulový determinant (věta ??).

Pro singulární matice lze zformulovat analogické podmínky: $\mathbf{A}$ je singulární, právě když neexistuje inverzní matice, právě když $\mathbf{AX} = \mathbf{B}$ nemá řešení pro některé matice $\mathbf{B}$, právě když $\operatorname{hod} \mathbf{A} < n$, právě když $\mathbf{A}$ má lineárně závislé řádky/sloupce, právě když $\mathbf{A}^T$ je singulární, právě když nelze $\mathbf{A}$ převést na $\mathbf{E}$ konečně mnoha kroky Gaussovy eliminační metody, právě když má nulový determinant.

6.47. Poznámka. Protože podle věty ?? je matice $\mathbf{A}$ regulární právě tehdy, když $\mathbf{A} \sim \mathbf{E}$, máme zaručeno, že metoda výpočtu inverzní matice neselže pro žádnou regulární matici. Jinými slovy, má-li matice inverzní matici, pak půjde provést eliminaci $(\mathbf{A}|\mathbf{E}) \sim (\mathbf{E}|\mathbf{B})$, což je podmínkou ke spuštění algoritmu ??.

6.48. Poznámka. Maticové rovnice z podmínky (4) lze řešit „vynásobením obou stran rovnice maticí $\mathbf{A}^{-1}$ zleva“. Tím se $\mathbf{AX} = \mathbf{B}$ převede na $\mathbf{X} = \mathbf{A}^{-1}\mathbf{B}$. Dále lze řešit maticové rovnice $\mathbf{XA} = \mathbf{B}$ (pro matice $\mathbf{X}, \mathbf{B} \in \mathbf{R}^{m,n}$) „vynásobením obou stran rovnice maticí $\mathbf{A}^{-1}$ zprava“. Tím dostáváme $\mathbf{X} = \mathbf{B}\mathbf{A}^{-1}$. Situace je tedy podobná jako s číselnou linární rovnicí $ax = b$ jen s tím rozdílem, že musíme mít na paměti, že není splněn komuntativní zákon součinu matic, takže $\mathbf{A}^{-1}\mathbf{B}$ nemusí být totéž jako $\mathbf{B}\mathbf{A}^{-1}$.

Mnoho maticových rovnic lze na maticové rovnice $\mathbf{AX} = \mathbf{B}$ nebo $\mathbf{XA} = \mathbf{B}$ převést, jak ukazuje následující příklad.

6.49. Příklad. Najdeme matici $\mathbf{X}$ takovou, aby byla splněna rovnice

$$\mathbf{A} \cdot \mathbf{X} - \mathbf{X} + 4\,\mathbf{A} = \mathbf{O},$$

kde $\mathbf{A} \in \mathbf{R}^{3,3}$ je matice z příkladu ?? a $\mathbf{O}$ je nulová matice stejného typu.

Hledaná matice musí být čtvercová typu $(3, 3)$, jinak by nebylo definováno sčítání. Rovnici postupně upravíme (dáváme si pozor na to, že nemusí platit komutativní zákon).

$$\mathbf{A} \cdot \mathbf{X} - \mathbf{X} = -4\,\mathbf{A} \quad \text{tj.} \quad \mathbf{A} \cdot \mathbf{X} - \mathbf{E} \cdot \mathbf{X} = -4\,\mathbf{A} \quad \text{tj.} \quad (\mathbf{A} - \mathbf{E}) \cdot \mathbf{X} = -4\,\mathbf{A}.$$

Pokud existuje matice $(\mathbf{A} - \mathbf{E})^{-1}$, pak po pronásobení obou stran rovnice touto maticí *zleva* dostáváme

$$\mathbf{X} = (\mathbf{A} - \mathbf{E})^{-1} \cdot (-4\,\mathbf{A}) = -4\,(\mathbf{A} - \mathbf{E})^{-1} \cdot \mathbf{A}.$$

Je tedy potřeba najít inverzní matici k matici $\mathbf{A}-\mathbf{E}$ (například metodou popsanou v příkladu ??). Nalezenou inverzní matici vynásobíme čtyřmi a nakonec provedeme maticové násobení $4\,(\mathbf{A}-\mathbf{E})^{-1}\cdot\mathbf{A}$ podle definice. Níže uvádíme jednotlivé mezivýpočty:

$$\mathbf{A}-\mathbf{E}=\begin{pmatrix}0&2&3\\-1&-1&1\\2&2&0\end{pmatrix},\quad (\mathbf{A}-\mathbf{E})^{-1}=\begin{pmatrix}-\frac{1}{2}&\frac{3}{2}&\frac{5}{4}\\\frac{1}{2}&-\frac{3}{2}&-\frac{3}{4}\\0&1&\frac{1}{2}\end{pmatrix},\quad 4\,(\mathbf{A}-\mathbf{E})^{-1}=\begin{pmatrix}-2&6&5\\2&-6&-3\\0&4&2\end{pmatrix}$$

$$\mathbf{X}=-4\,(\mathbf{A}-\mathbf{E})^{-1}\cdot\mathbf{A}=-\begin{pmatrix}-2&6&5\\2&-6&-3\\0&4&2\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\-1&0&1\\2&2&1\end{pmatrix}=\begin{pmatrix}-2&-6&-5\\-2&2&3\\0&-4&-6\end{pmatrix}.$$

6.50. Poznámka. Z věty ?? víme, že hodnost matice se může zmenšit, pokud ji vynásobíme nějakou maticí. Nyní ukážeme, že hodnost matice se nezmění, pokud ji vynásobíme regulární maticí. Připomeneme nejdříve větu ??, která říká, že každému eliminačnímu procesu $\mathbf{A}\sim\mathbf{B}$ přísluší matice $\mathbf{P}$ tak, že $\mathbf{B}=\mathbf{P}\cdot\mathbf{A}$. Tato věta se dá v jistém smyslu obrátit:

6.51. Věta. Nechť $\mathbf{A},\mathbf{B}\in\mathbf{R}^{m,n}$. Nechť $\mathbf{P}\in\mathbf{R}^{m,m}$ je regulární matice a nechť $\mathbf{B}=\mathbf{P}\cdot\mathbf{A}$. Pak $\mathbf{A}\sim\mathbf{B}$.

Důkaz. Protože $\mathbf{P}$ je regulární, je podle podmínky (5) z věty ?? $\mathbf{P} \sim \mathbf{E}$ a ze symetrie relace $\sim$ plyne též $\mathbf{E} \sim \mathbf{P}$. Tedy $(\mathbf{E} \mid \mathbf{A}) \sim (\mathbf{P} \mid \mathbf{X}) = \mathbf{P}(\mathbf{E} \mid \mathbf{A}) = (\mathbf{P} \mid \mathbf{PA}) = (\mathbf{P} \mid \mathbf{B})$. Stejnou eliminaci provedeme pouze s pravým blokem, tj. dostáváme $\mathbf{A} \sim \mathbf{B}$.

6.52. Věta. Nechť $\mathbf{A}$ je libovolná matice (ne nutně čtvercová) a $\mathbf{P}$, $\mathbf{Q}$ jsou regulární matice takové, že je definováno násobení $\mathbf{P} \cdot \mathbf{A}$ a $\mathbf{A} \cdot \mathbf{Q}$. Pak $\hod \mathbf{A} = \hod(\mathbf{P} \cdot \mathbf{A}) = \hod(\mathbf{A} \cdot \mathbf{Q})$. Jinými slovy: násobení regulární maticí nemění hodnost.

Důkaz. Označme $\mathbf{B} = \mathbf{P} \cdot \mathbf{A}$. Podle věty ?? je $\mathbf{A} \sim \mathbf{B}$, takže $\hod \mathbf{A} = \hod \mathbf{B}$ podle věty ??.

K důkazu $\hod \mathbf{A} = \hod(\mathbf{A} \cdot \mathbf{Q})$ stačí podle (5) věty ?? přejít k transponovaným maticím a použít předchozí výsledek společně s větou ??: $\hod(\mathbf{A} \cdot \mathbf{Q}) = \hod(\mathbf{A} \cdot \mathbf{Q})^T = \hod(\mathbf{Q}^T \cdot \mathbf{A}^T) = \hod \mathbf{A}^T = \hod \mathbf{A}$.

6.53. Věta. $\mathbf{A} \sim \mathbf{B}$ právě tehdy, když $\langle \mathrm{r}\colon \mathbf{A} \rangle = \langle \mathrm{r}\colon \mathbf{B} \rangle$.

Důkaz. Implikaci „je-li $\mathbf{A} \sim \mathbf{B}$, pak $\langle \mathrm{r}\colon \mathbf{A} \rangle = \langle \mathrm{r}\colon \mathbf{B} \rangle$“ jsme dokázali v odstavci ??. Nyní tedy předpokládáme $\langle \mathrm{r}\colon \mathbf{A} \rangle = \langle \mathrm{r}\colon \mathbf{B} \rangle$ a najdeme takový eliminační proces, který převede matici $\mathbf{A}$ na matici $\mathbf{B}$.

Nejprve najdeme schodovité matice s nenulovými řádky $\mathbf{A}'$ a $\mathbf{B}'$ takové, že $\mathbf{A} \sim \mathbf{A}'$ a $\mathbf{B} \sim \mathbf{B}'$. To je možné díky větě ??. Stačí tedy ukázat, že $\mathbf{A}' \sim \mathbf{B}'$. Z věty ?? plyne, že $\langle \mathrm{r}\colon \mathbf{A} \rangle = \langle \mathrm{r}\colon \mathbf{A}' \rangle$ a $\langle \mathrm{r}\colon \mathbf{B} \rangle = \langle \mathrm{r}\colon \mathbf{B}' \rangle$ a z předpokladu $\langle \mathrm{r}\colon \mathbf{A} \rangle = \langle \mathrm{r}\colon \mathbf{B} \rangle$ plyne $\langle \mathrm{r}\colon \mathbf{A}' \rangle = \langle \mathrm{r}\colon \mathbf{B}' \rangle$. Matice

$\mathbf{A}'$ i $\mathbf{B}'$ mají lineárně nezávislé řádky a jejich počet je v obou případech roven $k = \hod \mathbf{A} = \hod \mathbf{B} = \hod \mathbf{A}' = \hod \mathbf{B}'$. Každý řádek matice $\mathbf{B}'$ je lineární kombinací řádků matice $\mathbf{A}'$, takže existuje čtvercová matice $\mathbf{P}$ (koeficientů těchto lineárních kombinací), pro kterou je $\mathbf{P} \cdot \mathbf{A}' = \mathbf{B}'$. Z věty ?? plyne, že $\hod \mathbf{P} = k$, což je počet řádků matice $\mathbf{P}$. Takže $\mathbf{P}$ je podle věty ?? regulární. Po použití věty ?? vidíme, že $\mathbf{A}' \sim \mathbf{B}'$.

6.54. Příklad.* Jestliže $\mathbf{A} \sim \mathbf{B}$, pak podle věty ?? existuje matice $\mathbf{P}$ taková, že $\mathbf{B} = \mathbf{PA}$. Podívejme se, jak vypadá matice $\mathbf{P}$ v případě jednotlivých elementárních kroků Gaussovy eliminační metody.

(1) Nechť $\mathbf{B}$ vznikla z $\mathbf{A}$ prohozením i-tého řádku s j-tým. Snadno ověříme, že $\mathbf{B} = \mathbf{P}_1 \cdot \mathbf{A}$, kde $\mathbf{P}_1$ je čtvercová matice, která vznikla z $\mathbf{E}$ prohozením i-ého řádku s j-tým.

(2) Nechť $\mathbf{B}$ vznikla z $\mathbf{A}$ vynásobením i-tého řádku nenulovou konstantou α. Snadno ověříme, že $\mathbf{B} = \mathbf{P}_2 \cdot \mathbf{A}$, kde $\mathbf{P}_2$ je čtvercová matice, kerá vznikla z $\mathbf{E}$ vynásobením i-ého řádku konstantou α.

(3) Nechť $\mathbf{B}$ vznikla z $\mathbf{A}$ přičtením α-násobku j-tého řádku i-tému. Snadno ověříme, že $\mathbf{B} = \mathbf{P}_3 \cdot \mathbf{A}$, kde $\mathbf{P}_3$ je čtvercová matice, kerá vznikla z $\mathbf{E}$ záměnou nuly za prvek α na pozici i, j.

6.55. Definice. Matice typu $\mathbf{P}_1$, $\mathbf{P}_2$ a $\mathbf{P}_3$ z příkladu ?? se nazývají *elementární matice*.

6.56. Věta. Symbolem $\mathbf{A} \sim \mathbf{B}$ v této větě značíme skutečnost, že matice $\mathbf{B}$ vznikla z matice $\mathbf{A}$ konečně mnoha kroky Gaussovy eliminační metody, přičemž není dovolen krok vynechání nebo přidání nulového řádku. Platí: $\mathbf{A} \sim \mathbf{B}$ právě tehdy, když existuje regulární matice $\mathbf{P}$ taková, že $\mathbf{B} = \mathbf{P} \cdot \mathbf{A}$.

Důkaz. Implikace „je-li $\mathbf{P}$ regulární, pak $\mathbf{PA} \sim \mathbf{A}$“ je dokázána ve větě ??. Je ovšem potřeba důkaz věty projít znovu a uvědomit si, že nebylo nutné použít krok vynechání nebo přidání nulového řádku. Nyní dokážeme opačnou implikaci. Předpokládejme, že $\mathbf{A} \sim \mathbf{B}$. Pak

$$\mathbf{B} = \mathbf{C}_m \cdot (\mathbf{C}_{k-1} \cdots (\mathbf{C}_2 \cdot (\mathbf{C}_1 \cdot \mathbf{A})) \cdots) = (\mathbf{C}_m \cdot \mathbf{C}_{k-1} \cdots \mathbf{C}_2 \cdot \mathbf{C}_1) \cdot \mathbf{A} = \mathbf{P} \cdot \mathbf{A},$$

kde $\mathbf{C}_k$ je elementární matice jednoho z typů $\mathbf{P}_1$, $\mathbf{P}_2$ a $\mathbf{P}_3$, která „emuluje“ provedení k-tého kroku eliminační metody. Jednotlivé elementární matice jsou zřejmě regulární, protože mají lineárně nezávislé řádky. Matice $\mathbf{P}$, která je součinem těchto elementárních regulárních matic, je podle věty ?? regulární.

6.57. Poznámka. V následujících odstavcích budeme pracovat se skupinou vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}$ L a další skupinou vektorů $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_m \in L$, která vznikne jejich lineárními kombinacemi. Tedy

$$\boldsymbol{y}_1 = \alpha_{1,1}\boldsymbol{x}_1 + \cdots + \alpha_{1,n}\boldsymbol{x}_n, \quad \boldsymbol{y}_2 = \alpha_{2,1}\boldsymbol{x}_1 + \cdots + \alpha_{2,n}\boldsymbol{x}_n, \quad \ldots, \quad \boldsymbol{y}_m = \alpha_{m,1}\boldsymbol{x}_1 + \cdots + \alpha_{m,n}\boldsymbol{x}_n$$

Tyto rovnosti lze v souladu s poznámkou ?? zapsat jako maticový součin

$$\begin{pmatrix} \boldsymbol{y}_1 \\ \boldsymbol{y}_2 \\ \vdots \\ \boldsymbol{y}_m \end{pmatrix} = \mathbf{A} \cdot \begin{pmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \\ \vdots \\ \boldsymbol{x}_n \end{pmatrix}, \quad \text{stručně } \mathbf{Y} = \mathbf{A} \cdot \mathbf{X},$$

kde $\mathbf{A} = (\alpha_{i,j}) \in \mathbf{R}^{n,m}$, $\mathbf{X} = (\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_n)^T \in L^{n,1}$, $\mathbf{Y} = (\boldsymbol{y}_1, \boldsymbol{y}_2, \dots, \boldsymbol{y}_m)^T \in L^{m,1}$.

6.58. Věta. Označme $\mathbf{A} = (\alpha_{i,j}) \in \mathbf{R}^{n,m}$, $\mathbf{X} = (\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_n)^T \in L^{n,1}$, $\mathbf{Y} = (\boldsymbol{y}_1, \boldsymbol{y}_2, \dots, \boldsymbol{y}_m)^T \in L^{m,1}$ a nechť $\mathbf{Y} = \mathbf{A} \cdot \mathbf{X}$. Označme ještě $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_m \in \mathbf{R}^n$ řádky matice $\mathbf{A}$ a nechť $\boldsymbol{b} = (\beta_1, \beta_2, \dots, \beta_n)$ je nějaký vektor z $\mathbf{R}^n$ a $\boldsymbol{z} = \beta_1 \boldsymbol{y}_1 + \beta_2 \boldsymbol{y}_2 + \dots + \beta_m \boldsymbol{y}_m$. Pak platí
(1) $\boldsymbol{b} \in \langle \boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_m \rangle$ právě tehdy, když $\boldsymbol{z} \in \langle \boldsymbol{y}_1, \boldsymbol{y}_2, \dots, \boldsymbol{y}_m \rangle$.
(2) Jsou-li $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_n$ lineárně nezávislé v L, pak $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_m$ jsou lineárně nezávislé v $\mathbf{R}^n$ právě tehdy, když $\boldsymbol{y}_1, \boldsymbol{y}_2, \dots, \boldsymbol{y}_m$ jsou lineárně nezávislé v L.
(3) Jsou-li $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_n$ lineárně nezávislé, pak $\dim\langle \boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_m \rangle = \dim\langle \boldsymbol{y}_1, \boldsymbol{y}_2, \dots, \boldsymbol{y}_m \rangle$.
(4) Je-li $m = n$ a $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n$ jsou lineárně nezávislé, pak $\langle \boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_n \rangle = \langle \boldsymbol{y}_1, \boldsymbol{y}_2, \dots, \boldsymbol{y}_n \rangle$.

Důkaz. (1) Nechť $\boldsymbol{b} \in \langle \boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_m \rangle$, tedy $\boldsymbol{b} = \gamma_1 \boldsymbol{a}_1 + \gamma_2 \boldsymbol{a}_2 + \dots + \gamma_m \boldsymbol{a}_m$, tj. $\boldsymbol{b} = (\gamma_1, \gamma_2, \dots, \gamma_m) \cdot \mathbf{A}$. Protože $\mathbf{A} \cdot \mathbf{X} = \mathbf{Y}$, je $(\gamma_1, \gamma_2, \dots, \gamma_m) \cdot \mathbf{Y} = (\gamma_1, \gamma_2, \dots, \gamma_m) \cdot \mathbf{A} \cdot \mathbf{X} = \boldsymbol{b} \cdot \mathbf{X} = \boldsymbol{z}$.

Takže $\boldsymbol{z} \in \langle \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_m \rangle$ a lineární kombinace vektorů $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_m$, která tvoří $\boldsymbol{z}$, má stejné koeficienty, jako lineární kombinace vektorů $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m$, která tvoří $\boldsymbol{b}$.

Nechť nyní $\boldsymbol{z} \in \langle \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_m \rangle$, tedy $\boldsymbol{z} = (\gamma_1, \gamma_2, \ldots, \gamma_m) \cdot \mathbf{Y}$. Protože $\mathbf{A} \cdot \mathbf{X} = \mathbf{Y}$, musí být $\boldsymbol{b} \cdot \mathbf{X} = \boldsymbol{z} = (\gamma_1, \gamma_2, \ldots, \gamma_m) \cdot \mathbf{Y} = (\gamma_1, \gamma_2, \ldots, \gamma_m) \cdot \mathbf{A} \cdot \mathbf{X}$, takže je $\boldsymbol{b} = (\gamma_1, \gamma_2, \ldots, \gamma_m) \cdot \mathbf{A}$. Vektor $\boldsymbol{b}$ je tedy lineární kombinací řádků matice $\mathbf{A}$ s koeficienty $\gamma_1, \gamma_2, \ldots, \gamma_m$.

(2) Nechť nejprve jsou vektory $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m$ lineárně nezávislé. Označíme symbolem $\boldsymbol{o}$ nulový vektor v L a ukážeme, že lineární kombinace $(\gamma_1, \gamma_2, \ldots, \gamma_m) \cdot \mathbf{Y} = \boldsymbol{o}$ musí být pouze triviální. Při označení $\boldsymbol{b} = (\gamma_1, \gamma_2, \ldots, \gamma_m) \cdot \mathbf{A}$ je $\boldsymbol{o} = (\gamma_1, \gamma_2, \ldots, \gamma_m) \cdot \mathbf{A} \cdot \mathbf{X} = \boldsymbol{b} \cdot \mathbf{X}$. Lineární kombinace vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ je zde rovna nulovému vektoru. Protože jsou vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ lineárně nezávislé, musí být tato kombinace triviální, neboli $\boldsymbol{b} = (0, 0, \ldots, 0)$. Je tedy $(\gamma_1, \gamma_2, \ldots, \gamma_m) \cdot \mathbf{A} = (0, 0, \ldots, 0)$. Levá strana této rovnosti je lineární kombinace řádků matice $\mathbf{A}$ s koeficienty γ_i, která je rovna nulovému řádku. Protože jsou tyto řádky lineárně nezávislé, musí $\gamma_i = 0$ pro $i = 1, 2, \ldots, m$.

Jsou-li vektory $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m$ lineárně závislé, pak podle věty ?? existuje jeden vektor $\boldsymbol{a}_r$, který je lineární kombinací ostatních vektorů $\boldsymbol{a}_i$. Podobně jako v důkazu (1) lze ukázat, že vektor $\boldsymbol{y}_r$ je pak lineární kombinací ostatních vektorů $\boldsymbol{y}_i$ a tato lineární kombinace má stejné koeficienty. Takže i vektory $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_m$ jsou lineárně závislé.

(3) Bázi $\langle \boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m \rangle$ lze najít jako největší podmnožinu množiny řádků $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_i$. Bázi $\langle \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_m \rangle$ lze vybrat stejným způsobem z množiny vektorů $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_m$. Z vlastnosti (2) plyne, že obě tyto podmnožiny musí být stejně početné.

(4) Protože $\mathbf{Y} = \mathbf{A} \cdot \mathbf{X}$, je $\langle \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_n \rangle \subseteq \langle \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \rangle$. Protože $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ jsou lineárně nezávislé, je matice $\mathbf{A}$ regulární, takže $\mathbf{X} = \mathbf{A}^{-1} \cdot \mathbf{Y}$. Z této rovnosti plyne, že $\langle \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \rangle \subseteq \langle \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_n \rangle$, takže platí obě inkluze a uvedené lineární obaly se rovnají.

6.59. Poznámka.* Řádky matice $\mathbf{A}$ ve větě ?? jsou koeficienty lineárních kombinací, kterými měníme skupinu vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ na novou skupinu vektorů $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_m$. Speciálně, je-li $\mathbf{A}$ některá z elementárních matic $\mathbf{P}_1$, $\mathbf{P}_2$ a $\mathbf{P}_3$ z příkladu ??, pak je regulární a má tedy lineárně nezávislé řádky. Podle (2) předchozí věty to znamená, že lineární nezávislost skupiny vektorů se nezmění změnou jejich pořadí, vynásobením jednoho vektoru nenulovou konstantou, přičtením násobku vektoru k jinému nebo konečným opakováním těchto úkonů. Z vlastnosti (4) předchozí věty dále vyplývá, že uvedené modifikace skupiny vektorů nezmění jejich lineární obal. To nám připomíná věty ?? a ??, ale tam jsme pracovali jen s řádky matice, tedy s vektory z $\mathbf{R}^n$. Nyní říkáme totéž o vektorech z libovolného lineárního prostoru L.

6.60. Shrnutí. Součin matic $\mathbf{A} \cdot \mathbf{B}$ je definován /??/ jen pro matice, kde $\mathbf{A}$ má stejný počet sloupců jako $\mathbf{B}$ řádků. Součin matic není obecně komutativní ani pro čtvercové matice. Ovšem platí asociativní i distributivní zákon /??/.

Matice lze násobit i po blocích /??, ??/. Například součin matic $\mathbf{A}\cdot\mathbf{B}$ obsahuje ve sloupcích součiny matice $\mathbf{A}$ s jednotlivými sloupci matice $\mathbf{B}$ /??/.

Blokovým násobením matic je inspirován Strassenův algoritmus, který má složitost pouze $n^{2,8}$, zatímco složitost maticového součinu podle definice je n^3.

Existuje skupina matic, která s pevně danou čtvercovou maticí komutuje. Tato skupina tvoří podprostor všech čtvercových matic.

Iverzní matice ke čtvercové matici $\mathbf{A}$ ja taková čtvercová matice $\mathbf{A}^{-1}$ stejného typu, která musí splňovat $\mathbf{A}\cdot\mathbf{A}^{-1} = \mathbf{A}^{-1}\cdot\mathbf{A} = \mathbf{E}$ /??/, kde $\mathbf{E}$ je jednotková matice /??/. Inverzní matice je jediná /??/. Z jedné definiční rovnosti plyne druhá /??/. Matici, která má inverzní, nazýváme regulární /??/. Součin regulárních matic je matice regulární /??/. Mezi ekvivalentní podmínky s regularitou matice $\mathbf{A}$ patří: $\operatorname{hod}\mathbf{A}$ = počet řádků, r: $\mathbf{A}$ je lineárně nezávislá množina, maticová rovnice $\mathbf{AX} = \mathbf{B}$ má řešení pro každou pravou stranu, platí $\mathbf{A} \sim \mathbf{E}$ /??/.

Na výpočet inverzní matice je možné použít algoritmus /??/ založený na Gaussově eliminační metodě. Že metoda skutečně počítá inverzní matici plyne z tvrzení, že pokud $\mathbf{A} \sim \mathbf{B}$, pak existuje matice $\mathbf{P}$ tak, že $\mathbf{B} = \mathbf{P}\cdot\mathbf{A}$ /??/. Větu můžeme za podmínky regularity $\mathbf{P}$ zformulovat jako ekvivalenci /??/. V takovém případě je $\mathbf{P}$ součinem emelmentárních matic /??/.

Hodnost součinu matic je nejvýše rovna hodnosti jednotlivých činitelů /??/. Násobíme-li matici regulární maticí, hodnost se nezmění /??/.

Maticové násobení jsme použili k vyjádření přechodu jedné skupiny vektorů z L k lineárním kombinacím této skupiny vektorů. Odvodili jsme, že také na abstraktní vektory z L můžeme uplatnit kroky Gaussovy eliminační metody jako na řádky matice, přitom jejich lineární nezávislost a jejich lineární obal zůstávají v takovém případě zchovány /??/.

7. LU rozklad

7.1. Poznámka. V této krátké kapitole ukážeme, že každou regulární matici lze (až na případné prohození sloupců) zapsat jako součin matic **L** a **U**, kde **L** je dolní trojúhelníková matice (má nenulové prvky soustředěny v dolním trojúhelníku) a **U** je horní trojúhelníková matice. Tento rozklad se používá při numerickém řešení soustav lineárních rovnic /??/, zejména při větším počtu pravých stran.

Toto téma spadá spiše do numerické matematiky. Přesto jsem se rozhodl je sem zařadit, protože hlavní myšlenka LU rozkladu využívá důležitý poznatek, který byl vysloven v předchozí kapitole: jednotlivé kroky eliminační metody lze „emulovat“ násobením příslušnými regulárními maticemi zleva. Následující kapitoly nepředpokládají znalosti o LU rozkladu. Pokud tedy čtenář nemá zájem tuto záležitost poznat hlouběji, může bez uzardění tuto kapitolu přeskočit.

7.2. Definice. Nechť $\mathbf{A} = (a_{ij})$ je čtvercová matice. Matici **A** nazýváme *horní trojuhelníkovou*, pokud má pod diagonálou jen nulové prvky (nenulové prvky jsou soustředěny v „horním tojúhelníku“), tedy $a_{i,j} = 0$ pro $i > j$. Matici **A** nazýváme *dolní trojúhelníkovou*, pokud má nad diagonálou jen nulové prvky, tedy $a_{i,j} = 0$ pro $i < j$.

7.3. Věta. (1) Součin dvou dolních trojúhelníkových matic s jedničkami na diagonále je dolní trojúhelníková matice s jedničkami na diagonále.

(2) Je-li $\mathbf{L}$ dolní trojúhelníková matice s jedničkami na diagonále, pak je regulární a $\mathbf{L}^{-1}$ je také dolní trojúhelníková matice s jedničkami na diagonále.

Důkaz. (1) Stačí si uvědomit, jak funguje maticové násobení.
(2) Ukážeme, že eliminaci $(\mathbf{L}\,|\,\mathbf{E}) \sim (\mathbf{E}\,|\,\mathbf{L}^{-1}) = \mathbf{P}\cdot(\mathbf{L}\,|\,\mathbf{E})$ lze vždy provést, takže $\mathbf{L}$ je regulární. $\mathbf{P} = \mathbf{L}^{-1}$ je součin elmentárních matic Gaussovy eliminace. Po přímém chodu Gaussovy eliminační metody jistě vytvoříme z dolní trojúhelníkové matice $\mathbf{L}$ matici $\mathbf{E}$. Zpětný chod není nutné použít, neboť nad diagonálou se už nuly vyskytují a eliminací nejsou znehodnoceny. Na diagonále matice $\mathbf{L}$ zůstávají jedničky. Takže není potřeba ani prohazovat řádky, ani násobit řádky konstantou. Matice $\mathbf{P}$ je tedy součinem jen elematárních matic typu $\mathbf{P}_3$ pro $j < i$, tedy dolních trojúhelníkových matic s jedničkami na diagonále. Podle (1) je tedy $\mathbf{P} = \mathbf{L}^{-1}$ dolní trojúhelníková s jedničkami na diagonále.

7.4. Algoritmus. Je dána čtvercová matice $\mathbf{A} \in \mathbf{R}^{n,n}$. Popíšeme algoritmus vzniku matic $\mathbf{L}$ a $\mathbf{U}$, pro které platí $\mathbf{A} = \mathbf{L}\cdot\mathbf{U}$.

Matici $(\mathbf{A}\,|\,\mathbf{E})$ převedeme eliminací na $(\mathbf{U}\,|\,\mathbf{L}')$. Předpokládáme, že v eliminaci nejsme nuceni prohazovat řádky. Pouze přičítáme násobky řádků k řádkům *pod nimi*. Tím máme zaručeno, že $\mathbf{L}'$ je dolní trojúhelníková matice s jedničkami na diagonále.

Protože podle věty ?? existuje regulární čtvercová matice $\mathbf{P}$ taková, že

$$(\mathbf{U}\,|\,\mathbf{L}') = \mathbf{P}\cdot(\mathbf{A}\,|\,\mathbf{E}) = (\mathbf{P}\cdot\mathbf{A}|\,\mathbf{P})$$

dostáváme $\mathbf{L}' = \mathbf{P}$ a $\mathbf{U} = \mathbf{P} \cdot \mathbf{A} = \mathbf{L}' \cdot \mathbf{A}$, neboli $(\mathbf{L}')^{-1} \cdot \mathbf{U} = \mathbf{A}$. Pro hledanou matici $\mathbf{L}$ tedy platí $\mathbf{L} = (\mathbf{L}')^{-1}$. Matice $\mathbf{L}$ je podle věty ?? dolní trojúhelníková s jedničkami na diagonále.

7.5. Příklad. Platí

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 4 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 6 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -5 \\ 0 & 0 & 18 \end{pmatrix} = \mathbf{L}\mathbf{U},$$

protože

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 2 & 3 & 1 & 0 & 1 & 0 \\ 4 & 2 & 0 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -1 & -5 & -2 & 1 & 0 \\ 0 & 0 & 18 & 8 & -6 & 1 \end{array}\right) = (\mathbf{U} \,|\, \mathbf{L}'), \quad (\mathbf{L}')^{-1} = \left(\begin{array}{ccc} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 6 & 1 \end{array}\right).$$

7.6. Poznámka. Pokud se při eliminaci použité v algoritmu ?? vyskytne na diagonále (v místě pivota) nulový prvek, jsme nuceni prohodit řádky nebo sloupce. V takovém případě matice $\mathbf{A}$ nemá přímý rozklad na $\mathbf{L} \cdot \mathbf{U}$. Místo toho rozkládáme modifikovanou matici $\mathbf{A}'$, která obsahuje vhodně přehozené řádky nebo sloupce matice $\mathbf{A}$ tak, aby k problému výskytu nulového diagonálního prvku během eliminace nedošlo. Prohazovaní řádků lze emulovat násobením tzv. *permutační maticí* zleva a prohazování sloupců lze emulovat tzv. *permutační maticí* zprava. V následujících odstavcích je tato problematika rozvedena podrobněji.

7.7. Definice. Matice typu $\mathbf{P}_1$, $\mathbf{P}_2$ a $\mathbf{P}_3$ z příkladu ?? se nazývají *elementární matice Gaussovy eliminační metody*. Speciálně matice typu $\mathbf{P}_1$ se nazývají *elementární permutační matice*. Součin elementárních permutačních matic se nazývá *permutační matice*.

7.8. Věta. Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$ je libovolná matice a $\mathbf{P} \in \mathbf{R}^{n,n}$ je permutační matice. Pak $\mathbf{PA}$ se liší od matice $\mathbf{A}$ jen prohozením některých řádků. Dále matice $\mathbf{AP}$ se liší od matice $\mathbf{A}$ jen prohozením některých sloupců.

Důkaz. Jednotlivé elementární permutační matice prohazují při násobení zleva dvojici řádků. Součin takových matic způsobí prohození více dvojic řádků za sebou, tedy nová matice $\mathbf{PA}$ má prohozeny některé řádky. Totéž platí pro součin $\mathbf{AP}$ a pro sloupce.

7.9. Věta. Pro permutační matici platí, že $\mathbf{P}^{-1} = \mathbf{P}^T$.

Důkaz. Stačí si uvědomit, že každá elementární permutační matice $\mathbf{P}$ má uvedenou vlastnost, tedy pro ni platí $\mathbf{P}^{-1} = \mathbf{P}^T$. Dokonce je $\mathbf{P} = \mathbf{P}^T = \mathbf{P}^{-1}$. Nechť nyní $\mathbf{P} = \mathbf{C}_1\mathbf{C}_2 \cdots \mathbf{C}_k$, kde $\mathbf{C}_i$ jsou elementární permutační matice. Pak

$$\mathbf{P} \cdot \mathbf{P}^T = (\mathbf{C}_1\mathbf{C}_2 \cdots \mathbf{C}_k)(\mathbf{C}_1\mathbf{C}_2 \cdots \mathbf{C}_k)^T = (\mathbf{C}_1\mathbf{C}_2 \cdots \mathbf{C}_k)(\mathbf{C}_k^T \cdots \mathbf{C}_2^T \cdots \mathbf{C}_1^T) = \mathbf{E}$$

a analogicky $\mathbf{P}^T \cdot \mathbf{P} = \mathbf{E}$. je tedy $\mathbf{P}^{-1} = \mathbf{P}^T$.

7.10. Věta. Pro každou regulární matici $\mathbf{A} \in \mathbf{R}^{n,n}$ existuje permutační matice $\mathbf{P} \in \mathbf{R}^{n,n}$, dolní trojúhelníková matice $\mathbf{L} \in \mathbf{R}^{n,n}$ s jedničkami na diagonále a horní trojúhelníková matice $\mathbf{U} \in \mathbf{R}^{n,n}$ tak, že $\mathbf{AP} = \mathbf{LU}$.

Důkaz. Provedeme eliminaci $\mathbf{A} \sim \mathbf{U}$ jako v algoritmu ??. Pokud narazíme na nulový diagonální prvek, pak v místě tohoto prvku nemůže být celý řádek nulový, protože matice $\mathbf{A}$ je regulární. Prohodíme v eliminované matici sloupce tak, aby diagonální prvek byl nenulový. Toto prohození sloupců je možné podchytit maticovým násobením permutační matice zprava. Protože řádkové eliminační úpravy lze podchytit násobením odpovídaícími maticemi zleva, do součinu těchto matic se nám permutační matice „nemíchají“ a po dokončení eliminace dostáváme $\mathbf{L}'\mathbf{AP} = \mathbf{U}$. Při označení $\mathbf{L} = (\mathbf{L}')^{-1}$ dostáváme $\mathbf{AP} = \mathbf{LU}$.

7.11. Příklad. Pro následující matici $\mathbf{A}$ dostaneme při eliminaci na pozici $(2, 2)$ nulu. Je tedy:

$$\mathbf{AP} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 1 \\ 4 & 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 12/5 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 3 & 2 \\ 0 & -5 & 0 \\ 0 & 0 & -6 \end{pmatrix} = \mathbf{LU}.$$

V tomto případě není matice $\mathbf{A}$ rozložitelná na součin $\mathbf{LU}$ bez předchozího prohození jejích sloupců.

7.12. Věta. Pro každou regulární matici $\mathbf{A} \in \mathbf{R}^{n,n}$ existuje permutační matice $\mathbf{P} \in \mathbf{R}^{n,n}$, dolní trojúhelníková matice $\mathbf{L} \in \mathbf{R}^{n,n}$ s jedničkami na diagonále a horní trojúhelníková matice $\mathbf{U} \in \mathbf{R}^{n,n}$ tak, že $\mathbf{PA} = \mathbf{LU}$.

Důkaz. Provedeme eliminaci $\mathbf{A} \sim \mathbf{U}$ jako v algoritmu ??. Pokud narazíme na nulový diagonální prvek, pak pod tímto prvkem nemohou být samé nuly, protože matice $\mathbf{A}$ je regulární. Prohodíme v eliminované matici řádky tak, aby diagonální prvek byl nenulový. Toto prohození řádků je možné podchytit maticovým násobením permutační matice zleva. Protože řádkové eliminační úpravy jsou podchyceny také násobením odpovídajícími maticemi zleva, bohužel, permutační matice se nám do součinu „přimíchaly“ a nemáme jistotu, že je možné je v součinu přesunout doprava bez porušení vlastnosti, že zbytek zůstane dolní diagonální matice. Pomůže ale následující představa. V okamžiku, kdy rozhodneme o prohození řádků, se vátíme k původní matici $\mathbf{A}$ a prohodíme stejné řádky této matice. Pak eliminujeme znovu. Je zřejmé, že eliminace proběhne podobně, ale na nulový diagonální prvek už nyní nenarazíme. Pokračujeme v eliminaci dále. Narazíme-li později znovu na problém nulového prvku na diagonále, prohodíme odpovídající řádky znovu v matici $\mathbf{A}$ a znovu eliminaci provedeme od začátku.

Pokud provádíme eliminaci celého bloku $(\mathbf{A} \,|\, \mathbf{E}) \sim (\mathbf{U} \,|\, \mathbf{L}')$, pak není nutné se po prohození řádků vracet na začátek eliminace, ale stačí prohodit v tomto bloku jen jisté části řádků. Přesněji. Nechť $a_{k,k} = 0$ a rozhodli jsme k-tý řádek prohodit s $(k+j)$-tým. V dané chvíli je v pravém bloku v $(n+k)$-tém sloupci a ve všech dalších vrpavo od něj torzo ještě nezmě-

něné jednotkové matice. S tímto blokem při prohazování řádků nehýbeme, pouze prohodíme zkrácené řádky délky $(n+k-1)$. Pak je možné rovnou v eliminaci pokračovat.

7.13. Příklad. Najdeme LU rozklad matice $\mathbf{A}$ z příkladu ??.

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 2 & 4 & 1 & 0 & 1 & 0 \\ 4 & 2 & 0 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 0 & -5 & -2 & 1 & 0 \\ 0 & -6 & -12 & -4 & 0 & 1 \end{array}\right) \overset{2}{\underset{3}{\leftrightarrow}} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -6 & -12 & -4 & 1 & 0 \\ 0 & 0 & -5 & -2 & 0 & 1 \end{array}\right)$$

Při prohození druhého řádku s třetím jsme ponechali nezměněný předposlední a poslední sloupec pravého bloku. Platí:

$$\mathbf{P} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \mathbf{L} = \begin{pmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ -2 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 4 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}, \quad \mathbf{U} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & -6 & -12 \\ 0 & 0 & -5 \end{pmatrix}, \quad \mathbf{PA} =$$

7.14. Poznámka. Protože pro permutační matici $\mathbf{P}$ platí $\mathbf{P}^{-1} = \mathbf{P}^T$, což je také permutační matice, často se setkáváme s následujícími vzorci, které jsou důsledky předchozích dvou vět:

$$\mathbf{A} = \mathbf{LUP}, \qquad \mathbf{A} = \mathbf{PLU}.$$

První vzorec je důsledkem eliminace s výběrem pivota prohazováním sloupců a druhý je důsledkem eliminace s výběrem pivota prohazováním řádků.

7.15. Věta. Má-li matice $\mathbf{A} \in \mathbf{R}^{n,n}$ LU rozklad bez nutnosti prohodit sloupce/řádky matice $\mathbf{A}$, je tento rozklad jednoznačný. Je-li nutné prohodit sloupce/řádky v matici $\mathbf{A}$, pak pro každou možnou volbu prohození sloupců/řádků je LU rozklad jednoznačný.

Důkaz. Nechť $\mathbf{A} = \mathbf{LU} = \mathbf{L}_1\mathbf{U}_1$, tj. předpokládáme dva LU rozklady matice $\mathbf{A}$. Protože je podle věty ?? matice $\mathbf{L}$ regulární, můžeme rovnost pronásobit zleva maticí $\mathbf{L}^{-1}$ a dostáváme $\mathbf{L}^{-1}\mathbf{A} = \mathbf{U} = \mathbf{L}^{-1}\mathbf{L}_1\mathbf{U}_1$. Protože $\mathbf{A}$ i $\mathbf{L}^{-1}$ jsou regulární, je regulární i matice $\mathbf{U}$, která je jejich součinem. Analogicky se odvodí, že matice $\mathbf{U}_1$ je regulární, tedy má na diagonále nenulové prvky. Dále po označení $\mathbf{L}^{-1}\mathbf{L}_1 = \mathbf{L}'$, což je podle věty ?? dolní trojúhelníková matice s jedničkami na diagonále, dostáváme rovnost $\mathbf{U} = \mathbf{L}'\mathbf{U}_1$. Dá se ukázat pomocí věty ?? a přechodem k transponovaným maticím, že inverze horní trojúhelníkové matice je horní trojúhelníková a že součin horních trojúhelníkových matic je horní trojúhelníková. Takže $\mathbf{U}\mathbf{U}_1^{-1} = \mathbf{L}'\mathbf{U}_1\mathbf{U}_1^{-1} = \mathbf{L}'$ je horní trojúhelníková matice. Protože $\mathbf{L}'$ je zároveň dolní trojúhelníková, musí mít nenulové prvky pouze na diagonále. Tam má ale jedničky, takže $\mathbf{L}' = \mathbf{E}$. Platí tedy $\mathbf{U} = \mathbf{L}'\mathbf{U}_1 = \mathbf{E}\mathbf{U}_1 = \mathbf{U}_1$ Po dosazení do původního vztahu máme rovnost, $\mathbf{LU} = \mathbf{L}_1\mathbf{U}$, kterou pronásobíme zprava inverzí k $\mathbf{U}$ a dostáváme $\mathbf{L} = \mathbf{L}_1$.

7.16. Poznámka. V numerických metodách se používají efektivnější algoritmy, než zde popsaný ??. Při výpočtu LU rozkladu se v žádném případě dodatečně nepočítá $\mathbf{L} = (\mathbf{L}')^{-1}$, ale využije se toho, že $\mathbf{L}$ obsahuje přímo koeficienty eliminace (s opačným znaménkem).

Existují algoritmy LU rozkladu, které mají stejnou složitost jako maticové násobení. Takže při použití Strassenova algoritmu ?? máme složitost $n^{2,807}$.

7.17. Shrnutí. Regulární matici lze (až na prohození sloupců nebo řádků) zapsat jednoznačně jako součin horní a dolní trojúhelníkové matice příslušných vlastností /??, ??, ??, ??/.

8. Determinant

Determinant je číslo, které jistým způsobem charakterizuje čtvercovou matici a které se využívá například při výpočtech řešení soustav lineárních rovnic. Toto číslo má mnoho důležitých významů, se kterými se setkáme nejen v lineární algebře, ale i v jiných matematických disciplínách. Determinant se podle definice počítá z prvků matice poměrně komplikovaným způsobem. Než budeme schopni tuto definici formulovat, musíme si něco říci o permutacích. Na tomto pojmu je totiž definice determinantu založena.

8.1. Definice. Nechť M je konečná množina o n prvcích. *Permutace prvků množiny M* je uspořádaná n-tice prvků množiny M taková, že žádný prvek z množiny M se v ní neopakuje. Permutaci prvků množiny $M = \{1, 2, \ldots, n\}$ nazýváme stručně *permutací n prvků*.

8.2. Příklad. Uvedeme některé permutace pěti prvků: $(1, 2, 4, 5, 3)$, $(5, 4, 3, 2, 1)$, $(3, 5, 4, 1, 2)$. Uspořádanou pětici $(1, 2, 3, 2, 4)$ nepovažujeme za permutaci, protože se zde opakuje prvek 2.

8.3. Věta. Počet různých permutací n prvků je roven číslu $n!$.

Důkaz. Připomínáme, že $n! = n(n-1)(n-2)\cdots 2 \cdot 1$. Důkaz věty provedeme matematickou indukcí. Pro čtenáře, který se s takovou formou důkazu ještě nesetkal, nejprve vysvětlíme princip matematické indukce.

Matematickou indukcí dokazujeme tvrzení, které má platit pro všechna $n \in \mathbf{N}$. Postupujeme ve dvou krocích. Nejprve dokážeme toto tvrzení pro $n = 1$. Pak dokážeme tzv. indukční krok, který je formulován ve tvaru implikace: „jestliže tvrzení platí pro n, pak platí pro $n+1$“. Obhájíme-li platnost této implikace, máme dokázáno tvrzení pro všechna $n \in \mathbf{N}$. Vysvětlíme si, proč. V prvním kroku jsme dokázali, že tvrzení platí pro $n = 1$. Uplatníme nyní indukční krok ve tvaru „jestliže tvrzení platí pro $n = 1$, pak platí pro $n = 2$“. Tím máme zaručeno, že tvrzení platí pro $n = 2$. Zopakujeme indukční krok, tentokrát ve tvaru „jestliže tvrzení platí pro $n = 2$, pak platí pro $n = 3$“. To dokazuje platnost tvrzení pro $n = 3$. Opakovaným uplatněním indukčního kroku jsme schopni doložit platnost tvrzení pro libovolně velké n.

Tvrzení naší věty je: „počet různých permutací n prvků je roven číslu $n!$“. Dokážeme v prvním kroku pro $n = 1$, tj. „počet různých permutací jednoho prvku je roven číslu $1! = 1$“. O tom ale asi nikdo nepochybuje, nelze totiž vytvořit nic jiného než permutaci (1).

Nyní dokážeme indukční krok. Předpokládáme tedy, že počet různých permutací n prvků je roven číslu $n!$ a dokážeme, že počet různých permutací $n + 1$ prvků je roven číslu $(n + 1)!$. Prozkoumejme nejprve, kolik existuje permutací $n+1$ prvků, které mají v první složce zapsáno číslo 1. Je jich $n!$, protože zbylých n složek můžeme zaplnit čísly $\{2, 3, \ldots, n, n + 1\}$ a máme v tomto případě stejné množství možností, jako je počet permutací n prvků. Těch je podle indukčního předpokladu $n!$. Ze stejného důvodu existuje $n!$ různých permutací $n + 1$ prvků, které mají v první složce zapsáno číslo 2. Totéž platí pro čísla $3, 4, \ldots, n, n + 1$ v první složce permutace. Existuje tedy $(n + 1) \cdot n! = (n + 1)!$ různých permutací $n + 1$ prvků.

8.4. Příklad. Uvedeme si všechny permutace tří prvků. Podle věty ?? je jejich počet roven šesti. Hledané permutace jsou:

$$(1,2,3),\quad (1,3,2),\quad (2,1,3),\quad (2,3,1),\quad (3,1,2),\quad (3,2,1).$$

Zkusíme ještě zapsat všechny permutace čtyř prvků. Je jich 24.

$$\begin{array}{llllllll}
(1,2,3,4), & (1,2,4,3), & (1,3,2,4), & (1,3,4,2), & (1,4,2,3), & (1,4,3,2), & (2,1,3,4), & (2,1,4,3),\\
(2,3,1,4), & (2,3,4,1), & (2,4,1,3), & (2,4,3,1), & (3,2,1,4), & (3,2,4,1), & (3,1,2,4), & (3,1,4,2),\\
(3,4,2,1), & (3,4,1,2), & (4,2,3,1), & (4,2,1,3), & (4,3,2,1), & (4,3,1,2), & (4,1,2,3), & (4,1,3,2).
\end{array}$$

Kdybychom chtěli zapsat všechny permutace 50 prvků, po použití věty ?? bychom si to rychle rozmysleli. Těch permutací totiž je přibližně $3\cdot 10^{64}$. Kdyby se nám na jeden řádek vešla jedna permutace a na stránku 60 řádků, spotřebovali bychom $5\cdot 10^{62}$ stránek. Při oboustranném tisku váží 500 stránek asi jeden kilogram, takže bychom spotřebovali 10^{57} tun papíru. Kdyby tisk jedné stránky trval vteřinu, strávili bychom u tiskárny zhruba 10^{55} let. Jistě uznáte, že to daleko přesahuje veškeré lidské možnosti.

8.5. Definice. Nechť $(i_1, i_2, \ldots, i_n)$ je permutace n prvků. *Inverze* této permutace je taková dvojice (i_k, i_l), pro kterou platí $i_k > i_l$, a přitom $k < l$.

8.6. Příklad. Permutace $(1,2,3)$ nemá žádnou inverzi. Permutace $(1,3,2)$ má jednu inverzi, totiž dvojici $(3,2)$, pro kterou platí $3>2$. Jednotlivé inverze jsou na následujících permutacích vyznačeny obloučkem

$$(1,2,3),\quad (1,\overset{\frown}{3,2}),\quad (\overset{\frown}{2,1},3),\quad (\overset{\frown}{2,3,1}),\quad (\overset{\frown}{3,1,2}),\quad (\overset{\frown}{3,2,1}).$$

Jako cvičení doplňte obloučky (tj. jednotlivé inverze) ke všem permutacím čtyř prvků.

8.7. Definice. Pro každou permutaci $\pi=(i_1,\dots,i_n)$ definujeme *znaménko permutace* $\operatorname{sgn}\pi$ takto:

$$\operatorname{sgn}\pi=\begin{cases}+1 & \text{má-li } \pi \text{ sudý počet inverzí}\\ -1 & \text{má-li } \pi \text{ lichý počet inverzí}\end{cases}$$

8.8. Příklad. Permutace z příkladu ?? mají tato znaménka:

$$\begin{aligned}&\operatorname{sgn}(1,2,3)=+1,\quad \operatorname{sgn}(1,3,2)=-1,\quad \operatorname{sgn}(2,1,3)=-1,\\ &\operatorname{sgn}(2,3,1)=+1,\quad \operatorname{sgn}(3,1,2)=+1,\quad \operatorname{sgn}(3,2,1)=-1.\end{aligned}$$

Jako cvičení si rozmyslete, jak vypadají znaménka všech permutací čtyř prvků.

8.9. Věta. Prohození jediné dvojice prvků v permutaci způsobí změnu jejího znaménka.

Důkaz. Nechť $\pi = (\ldots, a, \ldots, b, \ldots)$ a $\pi_1 = (\ldots, b, \ldots, a, \ldots)$ jsou dvě permutace, které se liší jen prohozením prvků a, b. Ukážeme, že rozdíl počtu inverzí permutací π a π_1 je liché číslo.

Inverze, ve kterých se nevyskytuje ani a, ani b, zůstávají v obou permutacích stejné. Tvoří-li dvojice (a, b) z permutace π inverzi, pak (b, a) z permutace π_1 inverzi netvoří a naopak. Zatím jsme tedy zjistili, že se permutace π a π_1 liší o jednu inverzi, což je liché číslo. Ještě prozkoumáme všechny inverze, ve kterých vystupuje a nebo b s nějakým jiným prvkem. Ukážeme, že pokud tam dojde ke změně, pak jedině o sudý počet inverzí.

Uvažujme nějaký prvek x s menším indexem, než indexy prvků a i b, nějaký prvek y s větším indexem, než indexy prvků a i b a nějaký prvek z, který má index mezi indexy a a b. Názorně:

$$\pi = (\ldots, x, \ldots, a, \ldots, z, \ldots, b, \ldots, y, \ldots), \quad \pi_1 = (\ldots, x, \ldots, b, \ldots, z, \ldots, a, \ldots, y, \ldots).$$

Nemusejí v každém případě všechny tyto prvky existovat. Další rozbor tedy provedeme jen tehdy, pokud příslušný prvek existuje. Zabývejme se nejprve prvky x a y. Případné inverze mezi prvky (x, a), (x, b), (a, y) a (b, y) zůstanou po prohození prvků a, b v nezměněném stavu. Zajímavý je tedy jen prvek z.

Nechť nejprve $a < z < b$, tj. v permutaci π netvoří dvojice (a, z) ani (z, b) inverzi. Pak v permutaci π_1 vznikají dvě nové inverze (b, z) a (z, a), a to je sudé číslo. Nechť dále $b < z < a$,

pak v permutaci π máme dvě inverze, které v permutaci π_1 zanikají. Proběhla rovněž změna o sudý počet inverzí. Ještě může dojít k situaci $z < a$ a $z < b$. Pak v permutaci π dvojice (a, z) tvoří inverzi a dvojice (z, b) netvoří, zatímco v permutaci π_1 dvojice (b, z) tvoří inverzi a dvojice (z, a) netvoří. Počet inverzí se tedy v tomto případě nezměnil. Poslední případ $a < z$ a $b < z$ ověříme podobně, jako předchozí.

8.10. Definice. Nechť $\pi = (i_1, i_2, \ldots, i_n)$ je permutace n prvků. *Inverzní permutací k permutaci π* je permutace $(j_1, j_2, \ldots, j_n)$, pro kterou platí $j_{i_k} = k$ pro všechna $k \in \{1, 2, \ldots, n\}$. Tuto permutaci označujeme znakem π^{-1}.

8.11. Poznámka. Existuje několik možností, jak si představit inverzní permutaci k dané permutaci.

(1) Je-li v permutaci π na x-tém místě prvek y, pak v permutaci π^{-1} musí být na y-tém místě prvek x.

(2) Zapišme pod sebe permutaci π a permutaci $(1, 2, \ldots, n)$ takto:

$$\begin{pmatrix} i_1 & i_2 & i_3 & \ldots & i_n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}$$

a zaměňme pořadí sloupců této matice tak, abychom v prvním řádku měli vzestupně čísla $(1, 2, 3, \ldots, n)$. Pak ve spodním řádku je zapsána inverzní permutace k permutaci π. Uvažujme

kupříkladu permutaci $(3,4,2,6,1,5)$ a pišme:

$$\begin{pmatrix} 3 & 4 & 2 & 6 & 1 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 2 & 6 & 4 \end{pmatrix}.$$

Je tedy $(3,4,2,6,1,5)^{-1} = (5,3,1,2,6,4)$.

(3) Představme si šachovnici o rozměru $n \times n$ a rozestavme na ní n šachových věží tak, aby se vzájemně neohrožovaly. Takových rozestavení může být více a každé rozestavení můžeme popsat jednoznačně jako permutaci. V každém řádku i sloupci totiž stojí jediná věž a my můžeme číst rozestavení po řádcích takto: do první složky permutace napíšeme číslo sloupce, na kterém stojí věž z prvního řádku, do druhé složky číslo sloupce, na které stojí věž z druhého řádku atd. Dostáváme tak permutaci π. Pokud nyní čteme totéž rozestavení po sloupcích, tj. do první složky permutace napíšeme číslo řádku věže z prvního sloupce, do druhé složky číslo řádku věže z druhého sloupce atd., dostáváme permutaci π^{-1}.

(4) Permutace $(i_1, i_2, \ldots, i_n)$ vymezuje zobrazení $\pi\colon \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$, pro které platí $\pi(k) = i_k$. Toto zobrazení je zjevně prosté a na množinu $\{1,2,\ldots,n\}$. Inverzní zobrazení π^{-1} pak vymezuje inverzní permutaci. Platí $\pi \circ \pi^{-1} = \mathcal{I}$, kde $\mathcal{I}$ je identické zobrazení.

8.12. Věta. Nechť π je permutace n prvků. Pak π^{-1} má stejný počet inverzí, jako π.

Důkaz. Pro názornost si představíme inverzní permutaci způsobem (2) z poznámky ??. Zaměřme se na dva sloupce uvedené dvouřádkové matice před prohozením sloupců:

$$\begin{pmatrix} \dots, & x, & \dots, & y, & \dots \\ \dots, & a, & \dots, & b, & \dots \end{pmatrix}.$$

Protože jde o stav před prohozením sloupců, víme, že $a < b$. Pokud $x < y$, tj. (x, y) netvoří inverzi v permutaci π, zůstanou po prohození sloupců tyto dva sloupce za sebou ve stejném pořadí. Takže se nová inverze v permutaci π^{-1} nevytvoří. Pokud ale $x > y$, tj. (x, y) tvoří inverzi v permutaci π, pak po prohození sloupců budou tyto dva sloupce v opačném pořadí. Dvojice prvků (b, a) tedy bude tvořit inverzi v permutaci π^{-1}.

8.13. Věta. Permutace π a π^{-1} mají vždy stejná znaménka.

Důkaz. Věta je přímým důsledkem věty ??.

8.14. Poznámka. V předchozích definicích a větách jsme si řekli minimum toho, co potřebujeme vědět o permutacích, abychom pochopili definici determinantu a odvodili jednoduché vlastnosti determinantu. Ve skutečnosti se u permutací dá studovat ještě mnoho dalších vlastností, které zde nebudeme potřebovat.

8.15. Definice.* Nechť $\mathbf{A} = (a_{i,j}) \in \mathbf{R}^{n,n}$ je čtvercová matice. Číslo

$$\sum_{\pi=(i_1,i_2,\ldots,i_n)} \operatorname{sgn}\pi \cdot a_{1,i_1}\, a_{2,i_2} \cdots a_{n,i_n} \tag{8.1}$$

nazýváme *determinantem matice* $\mathbf{A}$ a značíme je $\det \mathbf{A}$. V uvedeném vzorci se sčítá přes všechny permutace n prvků, tj. jedná se podle věty ?? o $n!$ sčítanců.

8.16. Poznámka. Je možné, že vzorec z definice ?? je pro některé čtenáře málo srozumitelný. Pokusíme se jej proto v této poznámce trochu vysvětlit a zlidštit.

Představme si čtvercovou matici jako šachovnici rozměru $n \times n$ a pokusme se na ni rozmístit n šachových věží tak, aby se vzájemně neohrožovaly. Podle poznámky ??, odst. (3) je možné každé takové rozmístění popsat jednou permutací (pozice věží čteme po řádcích). Podle věty ?? vidíme, že existuje $n!$ různých permutací, tedy existuje $n!$ různých řešení této šachové úlohy. Pro každé řešení této úlohy zapíšeme odpovídající permutaci, zjistíme znaménko této permutace, nadzvedneme věžičky a zapíšeme si hodnoty prvků, na kterých ty figurky stojí, vynásobíme tyto hodnoty mezi sebou a výsledek ještě násobíme znaménkem permutace. Pak si tento výsledek uložíme do paměti. Až projdeme všech $n!$ možností rozmístění věží, získáme v paměti $n!$ sčítanců a ty sečteme. Výsledkem je determinant matice.

8.17. Příklad. Hledejme determinant matice z $\mathbf{R}^{3,3}$ tvaru

$$\mathbf{A} = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}.$$

Podle vzorce z definice ?? budeme sčítat přes všechny permutace tří prvků. Těch je podle věty ?? $3! = 6$. Zapíšeme všechny tyto permutace, jejich znaménka a odpovídající rozmístění „šachových věží“.

$\pi = (1,2,3)$, $\operatorname{sgn}\pi = +1$, $\begin{pmatrix} \textcircled{a_{1,1}} & a_{1,2} & a_{1,3} \\ a_{2,1} & \textcircled{a_{2,2}} & a_{2,3} \\ a_{3,1} & a_{3,2} & \textcircled{a_{3,3}} \end{pmatrix}$, sčítanec: $+ a_{1,1} \cdot a_{2,2} \cdot a_{3,3}$.

$\pi = (2,3,1)$, $\operatorname{sgn}\pi = +1$, $\begin{pmatrix} a_{1,1} & \textcircled{a_{1,2}} & a_{1,3} \\ a_{2,1} & a_{2,2} & \textcircled{a_{2,3}} \\ \textcircled{a_{3,1}} & a_{3,2} & a_{3,3} \end{pmatrix}$, sčítanec: $+ a_{1,2} \cdot a_{2,3} \cdot a_{3,1}$.

$\pi = (3,1,2)$, $\operatorname{sgn}\pi = +1$, $\begin{pmatrix} a_{1,1} & a_{1,2} & \textcircled{a_{1,3}} \\ \textcircled{a_{2,1}} & a_{2,2} & a_{2,3} \\ a_{3,1} & \textcircled{a_{3,2}} & a_{3,3} \end{pmatrix}$, sčítanec: $+ a_{1,3} \cdot a_{2,1} \cdot a_{3,2}$.

$$\pi = (3,2,1), \quad \operatorname{sgn}\pi = -1, \quad \begin{pmatrix} a_{1,1} & a_{1,2} & \textcircled{a_{1,3}} \\ a_{2,1} & \textcircled{a_{2,2}} & a_{2,3} \\ \textcircled{a_{3,1}} & a_{3,2} & a_{3,3} \end{pmatrix}, \quad \text{sčítanec:} \quad -a_{1,3}\cdot a_{2,2}\cdot a_{3,1}.$$

$$\pi = (2,1,3), \quad \operatorname{sgn}\pi = -1, \quad \begin{pmatrix} a_{1,1} & \textcircled{a_{1,2}} & a_{1,3} \\ \textcircled{a_{2,1}} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & \textcircled{a_{3,3}} \end{pmatrix}, \quad \text{sčítanec:} \quad -a_{1,2}\cdot a_{2,1}\cdot a_{3,3}.$$

$$\pi = (1,3,2), \quad \operatorname{sgn}\pi = -1, \quad \begin{pmatrix} \textcircled{a_{1,1}} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & \textcircled{a_{2,3}} \\ a_{3,1} & \textcircled{a_{3,2}} & a_{3,3} \end{pmatrix}, \quad \text{sčítanec:} \quad -a_{1,1}\cdot a_{2,3}\cdot a_{3,2}.$$

$$\det \mathbf{A} = a_{1,1}\,a_{2,2}\,a_{3,3} + a_{1,2}\,a_{2,3}\,a_{3,1} + a_{1,3}\,a_{2,1}\,a_{3,2} - a_{1,3}\,a_{2,2}\,a_{3,1} - a_{1,2}\,a_{2,1}\,a_{3,3} - a_{1,1}\,a_{2,3}\,a_{3,2}.$$

Tento vzorec se dá zapamatovat pomocí mnemotechnické pomůcky: nejprve násobíme prvky na hlavní diagonále, dále ve směrech rovnoběžných s hlavní diagonálou a součiny sčítáme. Pak násobíme prvky na vedlejší diagonále, dále ve směrech rovnoběžných s vedlejší diagonálou, přičemž tyto součiny odečítáme. Této „poučce o diagonálách“, která je použitelná jen pro matice typu $(3,3)$, říkáme *Sarrusovo pravidlo*. Toto populární pravidlo tedy není nic jiného než rozepsání definice determinantu pro matice z $\mathbf{R}^{3,3}$.

Pro matici typu $(4,4)$ bychom dostali při výpočtu determinantu podle definice $4! = 24$ sčítanců. Pro takovou matici se už těžko hledají mnemotechnické pomůcky. Má-li čtenář čas a místo na papíře, může se pokusit sestavit všechny permutace čtyř prvků, najít jejich

znaménka a sečíst odpovídající součiny. Pokud čtenář nemá čas nebo místo na papíře, udělá nejlíp, když si počká na další metodu na počítání determinantů, která bude vyžadovat daleko méně početních úkonů. Na druhé straně rozepsání vzorce pro determinant matice typu $(4,4)$ je užitečné cvičení pro pochopení definice determinantu.

8.18. Příklad. Podobně, jako v předchozím příkladě, odvodíme vzorec pro výpočet determinantu matice z $\mathbf{R}^{2,2}$.

$$\pi = (1,2), \quad \operatorname{sgn}\pi = +1, \quad \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}, \quad \pi = (2,1), \quad \operatorname{sgn}\pi = -1, \quad \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix},$$

$$\det \mathbf{A} = a_{1,1} \cdot a_{2,2} - a_{1,2} \cdot a_{2,1}.$$

Pro úplnost uvedeme ještě hodnotu determinantu matice $\mathbf{A} = (a_{1,1})$ typu $(1,1)$. Zřejmě je $\det \mathbf{A} = a_{1,1}$.

8.19. Definice. Nechť $\mathbf{A} = (a_{i,j}) \in \mathbf{R}^{n,n}$ je čtvercová matice. *Hlavní diagonála matice* $\mathbf{A}$ je skupina jejích prvků $a_{1,1}, a_{2,2}, \ldots, a_{n,n}$. *Vedlejší diagonála matice* $\mathbf{A}$ zahrnuje prvky $a_{1,n}, a_{2,n-1}, \ldots, a_{n,1}$. *Prvek pod hlavní diagonálou* je každý prvek $a_{i,j}$, pro který platí $i > j$. *Prvek nad hlavní diagonálou* je každý prvek $a_{i,j}$, pro který platí $i < j$.

8.20. Příklad. Nechť matice $\mathbf{A} \in \mathbf{R}^{n,n}$ má pod hlavní diagonálou jen nulové prvky. Matice tedy názorně vypadá takto:

$$\mathbf{A} = \begin{pmatrix} a_{1,1}, & a_{1,2}, & \dots, & a_{1,n-1}, & a_{1,n} \\ 0, & a_{2,2}, & \dots, & a_{2,n-1}, & a_{2,n} \\ 0, & 0, & \dots, & a_{3,n-1}, & a_{3,n} \\ & & \vdots & & \\ 0, & 0, & \dots, & 0, & a_{n,n} \end{pmatrix}. \tag{8.2}$$

Zkusíme spočítat $\det \mathbf{A}$.

V definici determinantu ?? se pracuje se součtem součinů $\operatorname{sgn} \pi \cdot a_{1,i_1} \cdot a_{2,i_2} \cdots a_{n,i_n}$. Pokud aspoň jeden z těchto činitelů je nulový, je nulový celý součin. V celkovém součtu nás zajímají jen nenulové součiny. Prozkoumejme, které to jsou. Z posledního řádku musíme vzít jen prvek $a_{n,n}$, protože všechny ostatní prvky v posledním řádku jsou nulové. Z předposledního řádku můžeme vzít jen prvek $a_{n-1,n-1}$, protože ostatní jsou nulové. Prvek $a_{n-1,n}$ nelze do součinu zahrnout, protože z posledního sloupce už v součinu máme prvek $a_{n,n}$ (věže by se vzájemně ohrožovaly). Analogickou úvahou zahrneme do součinu prvky $a_{n-2,n-2}, \dots, a_{2,2}, a_{1,1}$. Není tedy jiná možnost nenulového součinu, než součin $a_{1,1} \cdot a_{2,2} \cdots a_{n,n}$. Ten odpovídá permutaci $(1, 2, \dots, n)$, která nemá žádnou inverzi a její znaménko je tedy $+1$. Ostatní sčítanci z definice determinantu jsou nuloví. Proto $\det \mathbf{A} = a_{1,1} \cdot a_{2,2} \cdot a_{3,3} \cdots a_{n,n}$.

8.21. Věta.* Základní vlastnosti determinantu.

(V1) Jestliže se matice $\mathbf{B}$ liší od matice $\mathbf{A}$ jen prohozením jedné dvojice řádků, pak $\det \mathbf{B} = -\det \mathbf{A}$.

(V2) Jestliže matice $\mathbf{A}$ má dva stejné řádky, pak $\det \mathbf{A} = 0$.

V dalších vlastnostech (V3) až (V5) označujeme symbolem $\begin{pmatrix} \vdots \\ \boldsymbol{a}_i \\ \vdots \end{pmatrix}$ matice, které se liší pouze v i-tém řádku, zde označeném $\boldsymbol{a}_i$. V řádcích, které jsou vyznačeny tečkami, se jednotlivé

matice shodují.

$$\text{(V3)}\quad \det\begin{pmatrix}\vdots\\ \alpha\,\boldsymbol{a}_i\\ \vdots\end{pmatrix} = \alpha\,\det\begin{pmatrix}\vdots\\ \boldsymbol{a}_i\\ \vdots\end{pmatrix}.$$

$$\text{(V4)}\quad \det\begin{pmatrix}\vdots\\ \boldsymbol{a}_i\\ \vdots\end{pmatrix} + \det\begin{pmatrix}\vdots\\ \boldsymbol{b}_i\\ \vdots\end{pmatrix} = \det\begin{pmatrix}\vdots\\ \boldsymbol{a}_i+\boldsymbol{b}_i\\ \vdots\end{pmatrix}.$$

$$\text{(V5)}\quad \det\begin{pmatrix}\vdots\\ \boldsymbol{a}_i+\alpha\,\boldsymbol{a}_j\\ \vdots\end{pmatrix} = \det\begin{pmatrix}\vdots\\ \boldsymbol{a}_i\\ \vdots\end{pmatrix},\quad \text{kde } \boldsymbol{a}_j \text{ je nějaký jiný řádek téže matice.}$$

Důkaz. (V1) Součin $a_{1,i_1}\cdots a_{n,i_n}$ odpovídá ve vzorci pro výpočet $\det \mathbf{A}$ permutaci $\pi = (i_1, i_2, \ldots, i_n)$. Tentýž součin najdeme i ve vzorci pro výpočet $\det \mathbf{B}$, pouze bude odpovídat permutaci π', která vznikne z permutace π přehozením dvou prvků. To podle věty ?? znamená, že $\operatorname{sgn}\pi' = -\operatorname{sgn}\pi$. V každém z $n!$ sčítanců pro výpočet $\det \mathbf{B}$ tedy máme opačné znaménko, než ve sčítancích pro výpočet $\det \mathbf{A}$. Musí tedy být $\det \mathbf{B} = -\det \mathbf{A}$.

(V2) Prohodíme-li v matici $\mathbf{A}$ mezi sebou dva stejné řádky, dostáváme zase matici $\mathbf{A}$. Podle (V1) pro tuto matici platí $\det \mathbf{A} = -\det \mathbf{A}$, což nemůže být splněno jinak, než že $\det \mathbf{A} = 0$.

Vlastnosti (V3) a (V4) plynou přímo z definice determinantu:

$$\text{(V3)} \quad \sum \operatorname{sgn} \pi \, a_{1,j_1} \, a_{2,j_2} \cdots (\alpha \, a_{i,j_i}) \, a_{i+1,j_{i+1}} \cdots a_{n,j_n} = \alpha \sum \operatorname{sgn} \pi \, a_{1,j_1} \, a_{2,j_2} \cdots a_{i,j_i} \, a_{i+1,j_{i+1}}$$

$$\text{(V4)} \quad \sum \operatorname{sgn} \pi \, a_{1,j_1} \, a_{2,j_2} \cdots (a_{i,j_i} + b_{i,j_i}) \, a_{i+1,j_{i+1}} \cdots a_{n,j_n} =$$

$$= \sum \operatorname{sgn} \pi \, a_{1,j_1} \, a_{2,j_2} \cdots a_{i,j_i} \, a_{i+1,j_{i+1}} \cdots a_{n,j_n} + \sum \operatorname{sgn} \pi \, a_{1,j_1} \, a_{2,j_2} \cdots b_{i,j_i} \, a_{i+1,j_{i+1}} \cdots a$$

(V5) dokážeme použitím právě dokázaných vlastností:

$$\det \begin{pmatrix} \vdots \\ \boldsymbol{a}_j \\ \vdots \\ \boldsymbol{a}_i + \alpha \, \boldsymbol{a}_j \\ \vdots \end{pmatrix} \overset{\text{(V4)}}{=} \det \begin{pmatrix} \vdots \\ \boldsymbol{a}_j \\ \vdots \\ \boldsymbol{a}_i \\ \vdots \end{pmatrix} + \det \begin{pmatrix} \vdots \\ \boldsymbol{a}_j \\ \vdots \\ \alpha \, \boldsymbol{a}_j \\ \vdots \end{pmatrix} \overset{\text{(V3)}}{=} \det \begin{pmatrix} \vdots \\ \boldsymbol{a}_j \\ \vdots \\ \boldsymbol{a}_i \\ \vdots \end{pmatrix} + \alpha \det \begin{pmatrix} \vdots \\ \boldsymbol{a}_j \\ \vdots \\ \boldsymbol{a}_j \\ \vdots \end{pmatrix} \overset{\text{(V2)}}{=} \det$$

8.22. Poznámka. Vlastnosti (V1), (V3) a (V5) nám ukazují, jak se změní determinant, změníme-li matici pomocí Gaussovy eliminační metody. Prohození řádků změní znaménko, vynásobení řádku nenulovým číslem α způsobí, že se determinant α-krát zvětší a konečně přičtení α-násobku jiného řádku ke zvolenému řádku nezmění hodnotu determinantu. Jsme tedy schopni upravovat matice Gaussovou eliminační metodou, a přitom si poznamenávat, jak se mění determinant. Tím můžeme převést matici na tvar (8.2). O této matici víme, že má determinant roven součinu prvků na hlavní diagonále.

Uvědomme si, že tato metoda dává výraznou úsporu času a výpočetních prostředků při počítání determinantů. Představme si, že počítáme determinant matice typu (n, n). Při Gaussově eliminační metodě potřebujeme zhruba n operací na výrobu jednoho nulového prvku. Těch nul potřebujeme vytvořit zhruba $n^2/2$, takže k výpočtu determinantu nám stačí $n^3/2$ operací. Pro matici typu $(50, 50)$ to je zhruba 62 500 operací. Pokud bychom chtěli počítat determinant stejně velké matice přímo z definice, potřebovali bychom na to $50 \cdot 3 \cdot 10^{64}$ operací (viz komentář v příkladu ??). Není v silách žádné výpočetní techniky spočítat to v rozumném čase.

8.23. Příklad. Právě popsanou metodou spočítáme determinant matice

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 4 & -1 \\ 2 & 1 & 2 & 2 \\ 1 & 3 & 1 & 2 \\ 2 & 1 & 2 & 1 \end{pmatrix}.$$

V literatuře se pro $\det \mathbf{A}$ často používá značení $|\mathbf{A}|$. Níže tedy zapisujeme prvky jednotlivých matic mezi svislé čáry a tím dáváme na jevo, že počítáme determinant.

$$\begin{vmatrix} 1 & 2 & 4 & -1 \\ 2 & 1 & 2 & 2 \\ 1 & 3 & 1 & 2 \\ 2 & 1 & 2 & 1 \end{vmatrix} \overset{(1)}{=} \begin{vmatrix} 1 & 2 & 4 & -1 \\ 0 & -3 & -6 & 4 \\ 0 & 1 & -3 & 3 \\ 0 & -3 & -6 & 3 \end{vmatrix} \overset{(2)}{=} - \begin{vmatrix} 1 & 2 & 4 & -1 \\ 0 & 1 & -3 & 3 \\ 0 & -3 & -6 & 4 \\ 0 & -3 & -6 & 3 \end{vmatrix} \overset{(3)}{=} - \begin{vmatrix} 1 & 2 & 4 & -1 \\ 0 & 1 & -3 & 3 \\ 0 & 0 & -15 & 13 \\ 0 & 0 & -15 & 12 \end{vmatrix} \overset{(4)}{=} - \begin{vmatrix} 1 & 2 & 4 & -1 \\ 0 & 1 & -3 & 3 \\ 0 & 0 & -15 & 13 \\ 0 & 0 & 0 & -1 \end{vmatrix} = -(-15) \cdot (-1) = -15.$$

V kroku (1) jsme první řádek násobili -2 a přičítali k druhému, pak jsme první řádek násobili -1 a přičítali k třetímu a nakonec jsme první řádek násobili -2 a přičítali ke čtvrtému. Tyto operace podle (V5) nemění hodnotu determinantu. V kroku (2) jsme prohodili druhý řádek se třetím, což podle (V1) změní znaménko determinantu. Napsali jsme toto znaménko před determinant modifikované matice. V kroku (3) jsme druhý řádek násobili třemi a přičetli ke třetímu a čtvrtému. To podle (V5) nemění hodnotu determinantu. Konečně v kroku (4) jsme třetí řádek násobili -1 a přičetli ke čtvrtému. Tím dostáváme matici tvaru (8.2) z příkladu ??, o které víme, že má determinant roven součinu prvků na diagonále.

Upozorňujeme na častou začátečnickou chybu při počítání determinantů. V Gaussově eliminační metodě se většinou neklade důraz na to, který řádek od kterého odečítáme, protože

výsledný řádek můžeme kdykoli později násobit číslem -1. Při počítání determinantů to ale jedno není. Například v kroku (1) jsme od druhého řádku odečítali dvojnásobek prvního a výsledek psali na druhý řádek. Kdybychom od dvojnásobku prvního řádku odečítali druhý a výsledek psali do druhého řádku, dopustili bychom se chyby, která nám změní znaménko determinantu. Mnemotechnická pomůcka: píšeme-li výsledek součtu na i-tý řádek, pak i-tý řádek původní matice nesmí být v součtu násoben žádnou konstantou. Ostatní řádky mohou být násobeny libovolnou konstantou a přičítány k tomuto řádku. Je třeba si tedy uvědomit, že „přičtení násobku řádku $\boldsymbol{a}$ k řádku $\boldsymbol{b}$“ (korektní krok) není totéž, jako „přičtení řádku $\boldsymbol{a}$ k násobku řádku $\boldsymbol{b}$“ (nekorektní krok).

8.24. Příklad. Jednotková matice má determinant roven jedné. Jednotková matice je totiž tvaru (8.2), takže stačí pronásobit prvky na diagonále.

8.25. Příklad. Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$ má prvky na vedlejší diagonále rovny jedné a ostatní prvky jsou nulové. Spočítáme její determinant.

Prohodíme první řádek s posledním, druhý s předposledním atd. až se dostaneme k prostřednímu řádku. Pro liché n necháváme prostřední řádek na místě, pro sudé n prohodíme naposled mezi sebou řádky $n/2$ a $n/2+1$. V obou případech jsme udělali $[n/2]$ prohození (symbolem $[x]$ zde značíme celou část z x). Matici $\mathbf{A}$ jsme těmito úpravami převedli na jednotkovou matici $\mathbf{E}$. Podle předchozího příkladu je $\det \mathbf{E} = 1$, takže podle vlastnosti (V1) z věty ?? je $\det \mathbf{A} = (-1)^{[n/2]} \det \mathbf{E} = (-1)^{[n/2]}$.

8.26. Příklad. Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$ má nad vedlejší diagonálou nulové prvky. Spočítáme její determinant.

Prohazováním řádků, stejně jako v předchozím příkladě, převedeme matici na tvar (8.2). Prvky z vedlejší diagonály se při těchto úpravách přestěhují na hlavní diagonálu. Determinant takto upravené matice je podle příkladu ?? roven součinu prvků na diagonále, takže máme $\det \mathbf{A} = (-1)^{[n/2]} a_{1,n}\, a_{2,n-1} \cdots a_{n,1}$.

8.27. Věta. Čtvercová matice $\mathbf{A}$ je regulární právě tehdy, když $\det \mathbf{A} \neq 0$.

Důkaz. Všimneme si nejprve, že Gaussova eliminační metoda realizovaná kroky (V1), (V3) a (V5) podle předchozí věty ?? nemění „nulovost“ determinantu. Přesněji, je-li $\mathbf{A} \sim \mathbf{B}$, pak $\det \mathbf{A} \neq 0$ právě tehdy když $\det \mathbf{B} \neq 0$.

Je-li matice $\mathbf{A}$ regulární je podle věty ?? $\operatorname{hod} \mathbf{A} = n$. Po úpravě Gaussovou eliminační metodou na matici $\mathbf{B}$ tvaru (8.2) musejí být všechny prvky na diagonále nenulové, protože podle věty ?? je také $\operatorname{hod} \mathbf{B} = n$. To znamená, že $\det \mathbf{B} \neq 0$ a tedy i $\det \mathbf{A} \neq 0$.

Je-li matice $\mathbf{A}$ singulární, je $\operatorname{hod} \mathbf{A} < n$. Po úpravě Gaussovou eliminační metodou na matici $\mathbf{B}$ tvaru (8.2) bude existovat aspoň jeden řádek v matici $\mathbf{B}$ celý nulový. Nulový je tedy i diagonální prvek, takže $\det \mathbf{B} = 0$. Podle předchozího nutně musí být $\det \mathbf{A} = 0$.

8.28. Věta.* Nechť $\mathbf{A}$ je čtvercová matice. Pak $\det \mathbf{A} = \det \mathbf{A}^T$.

Důkaz. Součinu $a_{1,i_1}\, a_{2,i_2} \cdots a_{n,i_n}$ ze vzorce (8.1) pro $\det \mathbf{A}$ odpovídá permutace $\pi = (i_1, i_2, \dots,$ Uspořádáme činitele tohoto součinu podle velikosti druhého indexu a dostaneme $a_{j_1,1}\, a_{j_2,2} \cdots a_{j_n}$ kde pro permutaci $\pi_1 = (j_1, j_2, \dots, j_n)$ platí $\pi_1 = \pi^{-1}$. Právě takové součiny se objevují ve vzorci pro $\det \mathbf{A}^T$. Vidíme tedy, že oba vzorce $\det \mathbf{A}$ i $\det \mathbf{A}^T$ obsahují sumu stejných součinů, pouze permutace odpovídajících součinů je v prvním případě π a v druhém π^{-1}. Tyto permutace mají podle věty ?? stejný počet inverzí, takže i stejné znaménko. Musí tedy být $\det \mathbf{A} = \det \mathbf{A}^T$.

8.29. Poznámka. Z právě dokázané věty plyne, že vlastnosti vyjmenované ve větě ?? platí nejen pro řádky matice, ale též pro sloupce. Při počítání determinantu podle metody popsané v poznámce ?? můžeme tedy svobodně přecházet od řádkových úprav ke sloupcovým a zpět, protože vlastnosti (V1), (V3) a (V5) věty ?? platí nejen pro řádky, ale i pro sloupce (tzv. řádkově-sloupcová dualita).

8.30. Věta (o rozvoji determinantu podle r-tého řádku).* Nechť $\mathbf{A} = (a_{r,s}) \in \mathbf{R}^{n,n}$ je čtvercová matice a $\mathbf{A}_{i,j} \in \mathbf{R}^{n-1,n-1}$ jsou matice, které vzniknou z matice $\mathbf{A}$ vynecháním i-tého řádku a j-tého sloupce. Pak pro každé $r \in \{1, \dots, n\}$ platí

$$a_{r,1}\,(-1)^{r+1} \det \mathbf{A}_{r,1} + a_{r,2}\,(-1)^{r+2} \det \mathbf{A}_{r,2} + \cdots + a_{r,n}\,(-1)^{r+n} \det \mathbf{A}_{r,n} = \det \mathbf{A}. \tag{8.3}$$

Je-li dále $t \in \{1, \dots, n\}$, $t \neq r$, pak platí

$$a_{r,1}\,(-1)^{t+1} \det \mathbf{A}_{t,1} + a_{r,2}\,(-1)^{t+2} \det \mathbf{A}_{t,2} + \cdots + a_{r,n}\,(-1)^{t+n} \det \mathbf{A}_{t,n} = 0. \tag{8.4}$$

Důkaz (pro hloubavé čtenáře). Podívejme se na vzorec (8.1) pro $\det \mathbf{A}$. Seskupíme v něm všechny sčítance, které obsahují prvek $a_{1,1}$ k sobě, dále seskupíme k sobě sčítance, které obsahují prvek $a_{1,2}$ a tak dále až po poslední skupinu, ve které se vyskytují sčítanci s prvkem $a_{1,n}$. Tyto prvky ze součtů vytkneme. Pro s-tou skupinu sčítanců tedy máme:

$$\sum_{\pi=(s,i_2,\ldots,i_n)} \operatorname{sgn}\pi \cdot a_{1,s}\, a_{2,i_2} \cdots a_{n,i_n} = a_{1,s} \left(\sum_{\pi=(s,i_2,\ldots,i_n)} \operatorname{sgn}\pi \cdot a_{2,i_2} \cdots a_{n,i_n} \right) = *$$

Z permutace $\pi = (s, i_2, \ldots, i_n)$ prvků množiny $M = \{1, 2, \ldots, n\}$ vytvořme permutaci $\pi' = (i_2, \ldots, i_n)$ prvků množiny $M \setminus \{s\}$ tak, že odebereme první prvek z permutace π. Nová permutace π' má o $s-1$ méně inverzí než permutace π. (Nakreslete si všechny inverze spojené s prvkem s.) Pro znaménka permutací tedy platí $\operatorname{sgn}\pi = (-1)^{s-1} \operatorname{sgn}\pi' = (-1)^{s+1} \operatorname{sgn}\pi'$. Pokračujme nyní dále v našem výpočtu:

$$* = a_{1,s}\,(-1)^{1+s} \left(\sum_{\pi'=(i_2,\ldots,i_n)} \operatorname{sgn}\pi' \cdot a_{2,i_2} \cdots a_{n,i_n} \right) = a_{1,s}\,(-1)^{1+s} \det \mathbf{A}_{1,s}.$$

Determinant $\mathbf{A}$ je součtem všech skupin sčítanců pro $s = 1, 2, \ldots, n$, což dokazuje vzorec (8.3) pro $r = 1$.

Nechť nyní $r \neq 1$. Prohodíme r-tý řádek matice $\mathbf{A}$ s předchozím, pak jej prohodíme s dalším předcházejícím řádkem, atd. až dostaneme původně r-tý řádek na první řádek modifikované matice $\mathbf{B}$. K tomu potřebujeme provést $r-1$ prohození, takže platí $\det \mathbf{B} = (-1)^{r-1} \det \mathbf{A}$. Provedeme rozvoj determinantu matice $\mathbf{B}$ podle prvního řádku ($\mathbf{B}_{1,s}$ je matice, která vznikne z matice $\mathbf{B}$ vynecháním prvního řádku a s-tého sloupce):

$$\det \mathbf{B} = a_{r,1}\,(-1)^{1+1} \det \mathbf{B}_{1,1} + a_{r,2}\,(-1)^{2+1} \det \mathbf{B}_{1,2} + \cdots + a_{r,n}\,(-1)^{1+n} \det \mathbf{B}_{1,n}.$$

Protože $\det \mathbf{A} = (-1)^{r-1} \det \mathbf{B}$ a protože $\mathbf{B}_{1,s} = \mathbf{A}_{r,s}$, máme vzorec (8.3) dokázán.

Uvažujme $t \neq r$ a nahraďme t-tý řádek v matici $\mathbf{A}$ řádkem r-tým. Novou matici označme $\mathbf{C}$. Má dva stejné řádky, takže je $\det \mathbf{C} = 0$. Rozvoj tohoto determinantu podle t-tého řádku odpovídá vzorci (8.4).

8.31. Poznámka. Vzhledem k platnosti věty ?? platí analogická věta o rozvoji determinantu podle s-tého sloupce. Zkuste si ji zformulovat jako cvičení.

8.32. Definice. Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$. *Doplněk matice* $\mathbf{A}$ *v pozici* (i,j) je číslo $D_{i,j}$, definované vzorcem: $D_{i,j} = (-1)^{i+j} \det \mathbf{A}_{i,j}$, kde $\mathbf{A}_{i,j} \in \mathbf{R}^{n-1,n-1}$ je matice, která vznikne z matice $\mathbf{A}$ vynecháním i-tého řádku a j-tého sloupce.

8.33. Poznámka. Větu ?? lze při použití definice ?? a poznámky ?? přeformulovat. Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$ je čtvercová matice a $D_{i,j}$ jsou její doplňky. Nechť $r, s, t \in \{1, 2, \ldots, n\}$, $r \neq t$, $s \neq t$. Pak platí

$$\det \mathbf{A} = a_{r,1}\, D_{r,1} + a_{r,2}\, D_{r,2} + \cdots + a_{r,n}\, D_{r,n}, \quad 0 = a_{r,1}\, D_{t,1} + a_{r,2}\, D_{t,2} + \cdots + a_{r,n}\, D_{t,n},$$
$$\det \mathbf{A} = a_{1,s}\, D_{1,s} + a_{2,s}\, D_{2,s} + \cdots + a_{n,s}\, D_{n,s}, \quad 0 = a_{1,s}\, D_{1,t} + a_{2,s}\, D_{2,t} + \cdots + a_{n,s}\, D_{n,t}.$$

8.34. Příklad. Uvažujme matici $\mathbf{A}$ z příkladu ??. Provedeme rozvoj determinantu $\mathbf{A}$ podle prvního řádku.

$$\det \mathbf{A} = 1\cdot(-1)^{1+1}\cdot\begin{vmatrix} 1 & 2 & 2 \\ 3 & 1 & 2 \\ 1 & 2 & 1 \end{vmatrix} + 2\cdot(-1)^{1+2}\cdot\begin{vmatrix} 2 & 2 & 2 \\ 1 & 1 & 2 \\ 2 & 2 & 1 \end{vmatrix} + 4\cdot(-1)^{1+3}\cdot\begin{vmatrix} 2 & 1 & 2 \\ 1 & 3 & 2 \\ 2 & 1 & 1 \end{vmatrix} - 1\cdot(-1)^{1+4}\cdot\begin{vmatrix} 2 & 1 \\ 1 & 3 \\ 2 & 1 \end{vmatrix}$$
$$= 1 \cdot 5 + 2 \cdot 0 + 4 \cdot (-5) - 1 \cdot 0 = -15.$$

Vidíme, že jsme si při výpočtu moc nepomohli. Rozvoj determinantu podle řádku nebo sloupce matice typu (n, n) obecně vede na n determinantů matic, které mají o jediný řádek a sloupec méně. To není žádná výhra.

Kdybychom opakovaně prováděli rozvoj vzniklých determinantů podle řádku nebo sloupce, mohli bychom dojít až k maticím typu (1,1), u kterých je determinant přímo roven hodnotě prvku dané matice. Programátory může napadnout, že lze tedy větu o rozvoji determinantu

využít při implementaci výpočtu determinantu rekurzivním algoritmem. Ovšem pozor! Tento algoritmus potřebuje zcela stejné množství operací, jako při výpočtu determinantu přímo z definice. Jak už jsme si uváděli, při matici typu $(50, 50)$ se jedná zhruba o 10^{64} operací. Prakticky to znamená, že bychom se pravděpodobně výsledku nedočkali za celou dobu předpokládané existence naší sluneční soustavy a kdo ví, jestli by se dříve nezhroutil vesmír.

Můžete namítnout, k čemu že je metoda rozvoje determinantu dobrá? Pokud se v nějakém řádku nebo sloupci matice vyskytuje mnoho nul, můžeme zmenšit velikost matic, ze kterých počítáme determinant. Je-li na řádku nebo sloupci jediný nenulový prvek, dostáváme jedinou matici o jeden řádek a sloupec menší. V příkladu ?? jsme mohli například před provedením kroku (2) provést rozvoj determinantu podle prvního sloupce a dále pracovat jen s maticí typu $(3, 3)$. Před krokem (4) jsme mohli znovu provést rozvoj determinantu podle prvního sloupce:

$$\begin{vmatrix} 1 & 2 & 4 & -1 \\ 2 & 1 & 2 & 2 \\ 1 & 3 & 1 & 2 \\ 2 & 1 & 2 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 4 & -1 \\ 0 & -3 & -6 & 4 \\ 0 & 1 & -3 & 3 \\ 0 & -3 & -6 & 3 \end{vmatrix} = 1 \cdot \begin{vmatrix} -3 & -6 & 4 \\ 1 & -3 & 3 \\ -3 & -6 & 3 \end{vmatrix} = - \begin{vmatrix} 1 & -3 & 3 \\ -3 & -6 & 4 \\ -3 & -6 & 3 \end{vmatrix} =$$

$$= - \begin{vmatrix} 1 & -3 & 3 \\ 0 & -15 & 13 \\ 0 & -15 & 12 \end{vmatrix} = -1 \cdot \begin{vmatrix} -15 & 13 \\ -15 & 12 \end{vmatrix} = 15 \cdot 12 - 15 \cdot 13 = -15.$$

Výhoda se projeví výrazněji, pokud například čísla v prvním řádku či sloupci jsou nesoudělná a je výhodnější začít vyrábět nuly v jiném řádku nebo sloupci. Eliminační metodou v něm vytvoříme nuly a pak provedeme podle tohoto řádku nebo sloupce rozvoj determinantu.

8.35. Věta.* Nechť $\mathbf{A}$, $\mathbf{B}$ jsou čtvercové matice. Pak $\det \mathbf{A} \det \mathbf{B} = \det(\mathbf{A} \cdot \mathbf{B})$.

Důkaz (pro hloubavé čtenáře). Uvědomíme si, že lze matici $\mathbf{A}$ převést pouze řádkovými úpravami na matici $\mathbf{A}'$, která je tvaru (8.2). Navíc můžeme provádět pouze takové úpravy, které nemění determinant: přičítání násobku jiného řádku k řádku podle (V5) věty ?? nemění determinant a pokud potřebujeme prohodit řádky, pak okamžitě pronásobíme jeden z nich konstantou -1. Tyto operace skutečně stačí na převedení matice na tvar (8.2), a přitom máme zaručeno, že $\det \mathbf{A} = \det \mathbf{A}'$. Podle věty ?? existuje čtvercová matice $\mathbf{P}$, pro kterou platí

$$\mathbf{A}' = \mathbf{P} \cdot \mathbf{A}.$$

Dále převedeme matici $\mathbf{B}$ na matici $\mathbf{B}'$ tvaru (8.2) pouze sloupcovými úpravami takovými, které nemění determinant. Máme tedy $\det \mathbf{B} = \det \mathbf{B}'$ a navíc podle poznámky ?? existuje matice $\mathbf{Q}$ taková, že

$$\mathbf{B}' = \mathbf{B} \cdot \mathbf{Q}.$$

Platí

$$\det \mathbf{A} \det \mathbf{B} = \det \mathbf{A}' \det \mathbf{B}' = \det(\mathbf{A}' \cdot \mathbf{B}').$$

Poslední rovnost ověříme z definice maticového násobení a využijeme toho, že obě matice $\mathbf{A}'$ i $\mathbf{B}'$ jsou tvaru (8.2). Matice $\mathbf{A}' \cdot \mathbf{B}'$ je také tvaru (8.2) a pro její diagonální prvky $g_{i,i}$ platí, že $g_{i,i} = a'_{i,i}\, b'_{i,i}$. Protože se determinanty matic tvaru (8.2) počítají jako součin prvků na diagonále, máme skutečně $\det \mathbf{A}' \det \mathbf{B}' = \det(\mathbf{A}' \cdot \mathbf{B}')$.

Na matici $\mathbf{A} \cdot \mathbf{B}$ provedeme stejné řádkové a sloupcové úpravy, jako jsme provedli na matice $\mathbf{A}$ resp. $\mathbf{B}$. Dostaneme matici $\mathbf{A}' \cdot \mathbf{B}'$, protože

$$\mathbf{P} \cdot (\mathbf{A} \cdot \mathbf{B}) \cdot \mathbf{Q} = (\mathbf{P} \cdot \mathbf{A}) \cdot (\mathbf{B} \cdot \mathbf{Q}) = \mathbf{A}' \cdot \mathbf{B}'.$$

Provedené řádkové a sloupcové úpravy nemění determinant, takže matice $\mathbf{A}' \cdot \mathbf{B}'$ má stejný determinant jako matice $\mathbf{A} \cdot \mathbf{B}$. Dostáváme výsledek

$$\det \mathbf{A} \det \mathbf{B} = \det \mathbf{A}' \det \mathbf{B}' = \det(\mathbf{A}' \cdot \mathbf{B}') = \det(\mathbf{A} \cdot \mathbf{B}).$$

8.36. Věta. Nechť $\mathbf{A} = \mathbf{L}\mathbf{U}$ je LU rozklad matice $\mathbf{A}$. Pak $\det \mathbf{A}$ je roven součinu diagonálních prvků matice $\mathbf{U}$.

Důkaz. Podle věty ?? je $\det \mathbf{A} = \det \mathbf{L} \cdot \det \mathbf{U}$. Protože $\det \mathbf{L} = 1$ (má na diagonále pouze jedničky), je $\det \mathbf{A} = \det \mathbf{U}$ což je podle příkladu ?? součin diagonálních prvků matice $\mathbf{U}$.

8.37. Věta. Nechť $\mathbf{A}$ je regulární matice. Pak $\det \mathbf{A}^{-1} = 1/\det \mathbf{A}$.

Důkaz. Stačí použít větu ?? na součin $\mathbf{A} \cdot \mathbf{A}^{-1} = \mathbf{E}$, tedy $\det \mathbf{A} \cdot \det \mathbf{A}^{-1} = \det \mathbf{E} = 1$. Vydělením obou stran rovnice číslem $\det \mathbf{A}$ (které je podle věty ?? nenulové) dostáváme dokazovaný vzorec.

8.38. Věta. Je-li $\mathbf{A} \in \mathbf{R}^{n,n}$ regulární, pak

$$\mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}}\, \mathbf{D}^T,$$

kde $\mathbf{D} = (D_{i,j})$ je matice doplňků $\mathbf{A}$ v pozicích (i, j).

Důkaz. Protože je $\mathbf{A}$ regulární, má nenulový determinant, takže ve vzorci nedělíme nulou. Musíme ověřit, že pro matici $\mathbf{A}^{-1}$ vypočítanou z uvedeného vzorce, platí $\mathbf{A} \cdot \mathbf{A}^{-1} = \mathbf{E}$. Je-li $\mathbf{D} = (D_{i,j})$, pak samozřejme je $\mathbf{D}^T = (D_{j,i})$. Podle definice součinu matic ?? vypočítáme prvek $e_{i,k}$ matice $\mathbf{A} \cdot \mathbf{A}^{-1}$:

$$e_{i,k} = \sum_{j=1}^{n} a_{i,j}\, \frac{1}{\det \mathbf{A}}\, D_{k,j} = \frac{1}{\det \mathbf{A}} \left(a_{i,1} D_{k,1} + a_{i,2} D_{k,2} + \cdots + a_{i,n} D_{k,n}\right) = \begin{cases} \dfrac{1}{\det \mathbf{A}} \det \mathbf{A} = 1 & \text{pro} \\ \dfrac{1}{\det \mathbf{A}} \cdot 0 = 0 & \text{pro} \end{cases}$$

Zde jsme využili větu o rozvoji determinantu podle i-tého řádku, viz poznámku ??. Zjišťujeme, že prvky $e_{i,k}$ jsou skutečně prvky jednotkové matice ??. Rovnost $\mathbf{A}^{-1} \cdot \mathbf{A} = \mathbf{E}$ bychom dokazovali podobně. Použili bychom větu o rozvoji i-tého sloupce namísto řádku.

8.39. Poznámka. Věta ?? kromě teoretických důsledků, které uvidíme později, nám také dává návod, jak vypočítat inverzní matici k matici $\mathbf{A}$. Je to vlastně vedle v algoritmu ??, který využívá eliminační metodu, další způsob hledání inverzní matice. Můžeme ji říkat „metoda hledání inverzní matice pomocí doplňků“. Uvědomíme si ale, že pro velké matice je eliminační metoda podstatně účelnější než metoda pomocí doplňků, která vyžaduje spočítat n^2 determinantů matic typu $(n-1, n-1)$ a ještě spočítat $\det \mathbf{A}$. V následujících příkladech si proto tuto metodu ilustrujeme jen na malých maticích.

8.40. Příklad. Najdeme inverzní matici k matici

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Označme $\mathbf{D}$ matici doplňků k matici $\mathbf{A}$. V tomto případě se doplňky dobře počítají, protože obsahují determinanty matic typu $(1,1)$:

$$\mathbf{D} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}, \quad \mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}} \mathbf{D}^T = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

8.41. Příklad. Najdeme inverzní matici ke stejné matici, jako v příkladu ??, tj. k matici

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ -1 & 0 & 1 \\ 2 & 2 & 1 \end{pmatrix}.$$

Doplňky nyní budeme počítat z determinantů matic typu $(2,2)$, což už nám dá trochu práce.

$$\mathbf{D} = \begin{pmatrix} +\begin{vmatrix} 0 & 1 \\ 2 & 1 \end{vmatrix} & -\begin{vmatrix} -1 & 1 \\ 2 & 1 \end{vmatrix} & +\begin{vmatrix} -1 & 0 \\ 2 & 2 \end{vmatrix} \\ -\begin{vmatrix} 2 & 3 \\ 2 & 1 \end{vmatrix} & +\begin{vmatrix} 1 & 3 \\ 2 & 1 \end{vmatrix} & -\begin{vmatrix} 1 & 2 \\ 2 & 2 \end{vmatrix} \\ +\begin{vmatrix} 2 & 3 \\ 0 & 1 \end{vmatrix} & -\begin{vmatrix} 1 & 3 \\ -1 & 1 \end{vmatrix} & +\begin{vmatrix} 1 & 2 \\ -1 & 0 \end{vmatrix} \end{pmatrix} = \begin{pmatrix} -2 & 3 & -2 \\ 4 & -5 & 2 \\ 2 & -4 & 2 \end{pmatrix},$$

$$\det \mathbf{A} = -2, \qquad \mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}}\, \mathbf{B}^T = -\frac{1}{2} \begin{pmatrix} -2 & 4 & 2 \\ 3 & -5 & -4 \\ -2 & 2 & 2 \end{pmatrix}.$$

Výsledek můžeme srovnat s výsledkem v příkladu ??.

8.42. Příklad. Matici $\mathbf{A} \in \mathbf{R}^{2n,2n}$ rozdělme na bloky typu (n, n):

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_1 & \mathbf{A}_2 \\ \mathbf{A}_3 & \mathbf{A}_4 \end{pmatrix}.$$

Ukážeme, že obecně neplatí $\det \mathbf{A} = \det \mathbf{A}_1 \det \mathbf{A}_4 - \det \mathbf{A}_2 \det \mathbf{A}_3$.

Zvolme matici

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Ta má zřejmě determinant roven mínus jedné. Přitom $\det \mathbf{A}_1 \det \mathbf{A}_4 - \det \mathbf{A}_2 \det \mathbf{A}_3 = 0 - 0 = 0$.

Že uvedený blokový vzorec neplatí, nás může napadnout i z počtu součinů, které obsahuje definice determinantu. Determinant matice z $\mathbf{R}^{2n,2n}$ obsahuje $(2n)!$ součinů, zatímco blokový vzorec obsahuje jen $2(n!)^2$ součinů. To je zcela jiné číslo.

8.43. Příklad. Matici $\mathbf{A} \in \mathbf{R}^{n,n}$ rozdělme na bloky tak, že $\mathbf{A}_1$ a $\mathbf{A}_4$ jsou čtvercové matice:

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_1 & \mathbf{A}_2 \\ \mathbf{O} & \mathbf{A}_4 \end{pmatrix},$$

přitom $\mathbf{O}$ je nulová matice. Ukážeme, že pak $\det \mathbf{A} = \det \mathbf{A}_1 \det \mathbf{A}_4$.

Nechť blok $\mathbf{A}_1$ je typu (m, m), kde $m < n$. V matici $\mathbf{A}$ lze převést řádkovými úpravami Gaussovy eliminační metody blok $\mathbf{A}_1$ na schodovitou matici. Dá se to navíc provést tak, že matice $\mathbf{A}$ se změní v matici $\mathbf{A}' = (a'_{i,j})$ se stejným determinantem a pracujeme jen s prvními m řádky matice $\mathbf{A}$. Podle ?? platí $\det \mathbf{A}_1 = a'_{1,1} \cdot a'_{2,2} \cdots a'_{m,m}$. Dokazovaný vzorec je pak výsledkem opakovaného rozvoje determinantu matice $\mathbf{A}'$ podle prvního sloupce, podle druhého sloupce, atd. až podle m-tého sloupce.

8.44. Věta. Nechť matice $\mathbf{A} \in \mathbf{R}^{n,n}$ je rozdělena do bloků

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_{1,1} & \mathbf{A}_{1,2} & \mathbf{A}_{1,3} & \dots & \mathbf{A}_{1,k} \\ \mathbf{O} & \mathbf{A}_{2,2} & \mathbf{A}_{2,3} & \dots & \mathbf{A}_{2,k} \\ \mathbf{O} & \mathbf{O} & \mathbf{A}_{3,3} & \dots & \mathbf{A}_{3,k} \\ & & & \dots & \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \dots & \mathbf{A}_{k,k} \end{pmatrix}$$

tak, že diagonální bloky $\mathbf{A}_{i,i}$ jsou čtvercové a $\mathbf{O}$ značí nulové bloky (obecně různých typů). Pak

$$\det \mathbf{A} = \det \mathbf{A}_{1,1} \cdot \det \mathbf{A}_{2,2} \cdots \det \mathbf{A}_{k,k}.$$

Důkaz. Analogicky, jako v příkladu ??. Má-li se to provést pořádně, je potřeba použít indukci podle k, přičemž argumenty v příkladu ?? poslouží pro indukční krok.

8.45. Shrnutí. Determinant čtvercové matice je definován jako součet součinů prvků matice opatřených jistým znaménkem. Podrobněji viz ??.

Determinant je možné vypočítat i rekurzivním algoritmem pomocí věty o rozvoji determinantu podle řádku či sloupce /??, ??/.

Determinant se nezmění, pokud modifikujeme matici tak, že k jednomu řádku/sloupci přičítáme α-násobek řádku/sloupce jiného. Násobíme-li jeden řádek/sloupec nenulovou konstantou, stejnou konstantou je násoben determinant. Prohodíme-li dva řádky/sloupce, determinant změní znaménko /??/. Díky těmto vlastnostem můžeme hlídat změny v determinantu při všech krocích Gaussovy eliminační metody. Ta nám umožní převést matici na schodovitou, tedy horní trojúhelníkovou matici. Ta má determinant roven součinu prvků na diagonále /??/. To nám dává metodu na počítání determinantů pomocí Gaussovy eliminační metody. Tato metoda je výpočtově výrazně méně náročná než užití definice nebo rekurzivního algoritmu, který vychází z věty o rozvoji /??/.

Determinant matice je nenulový, právě když je matice regulární /??/.

Determinant součinu matic je roven součinu determinantů /??/.

Inverzní matici můžeme počítat jako matici doplňků /??/ transponovanou a násobenou převrácenou hodnotou determinantu /??/. To není efektivní metoda, ale má své teoretické důsledky, například při důkazu Cramerova pravidla /??/ z následující kapitoly.

9. Soustavy lineárních rovnic

9.1. Definice. Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$ je matice reálných čísel, nechť dále $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)^T$ je sloupcový vektor symbolů a $\boldsymbol{b} = (b_1, b_2, \ldots, b_m)^T \in \mathbf{R}^{m,1}$ je sloupcový vektor reálných čísel. Pak maticovou rovnost

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

navýváme *soustavou m lineárních rovnic o n neznámých*. Matici $\mathbf{A}$ nazýváme *maticí soustavy* a vektor $\boldsymbol{b} = (b_1, \ldots, b_m)^T$ nazýváme *vektorem pravých stran*. Připíšeme-li k matici soustavy do dalšího sloupce vektor $\boldsymbol{b}$ oddělený (pouze pro přehlednost) svislou čarou, dostáváme matici $(\mathbf{A}|\boldsymbol{b}) \in \mathbf{R}^{m,n+1}$, kterou nazýváme *rozšířenou maticí soustavy*.

9.2. Definice. *Řešením soustavy* $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ je takový vektor $\boldsymbol{v} = (\alpha_1, \alpha_2, \ldots, \alpha_n)^T \in \mathbf{R}^{n,1}$, pro který platí: dosadíme-li hodnoty α_i za symboly x_i, pak je splněna požadovaná maticová rovnost, tj.

$$\mathbf{A} \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}. \tag{9.1}$$

Řešit soustavu $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ znamená nalézt všechna její řešení, tj. nalézt podmnožinu $\mathbf{R}^{n,1}$ všech řešení této soustavy.

9.3. Poznámka. Ačkoli přesně řečeno je množina řešení podmnožinou sloupcových vektorů $\mathbf{R}^{n,1}$, často složky těchto řešení nakonec píšeme do řádků (viz izomorfismus zmíněný v poznámce ??). Mluvíme tedy o množině řešení jako o podmnožině $\mathbf{R}^n$. Jinými slovy, nedojde-li k nedorozumění, zapisujeme jednotlivá řešení soustavy $\boldsymbol{v} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ jako prvky z $\mathbf{R}^n$.

9.4. Věta (Frobeniova).* Soustava $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ má řešení právě tehdy, když $\operatorname{hod}\mathbf{A} = \operatorname{hod}(\mathbf{A}|\boldsymbol{b})$, tj. když hodnost matice soustavy se rovná hodnosti rozšířené matice soustavy.

Důkaz. Vektor $\boldsymbol{v} = (\alpha_1, \ldots, \alpha_n)^T$ je řešením soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ právě tehdy, když platí (9.1). To znamená, že sloupec $\boldsymbol{b}$ je lineární kombinací sloupců matice $\mathbf{A}$ s koeficienty $\alpha_1, \alpha_2, \ldots, \alpha_n$. To platí právě tehdy, když

$$\operatorname{hod}\begin{pmatrix}\mathbf{A}^T\\ \boldsymbol{b}^T\end{pmatrix} = \operatorname{hod}\mathbf{A}^T.$$

Protože platí věta ??, je Frobeniova věta dokázána.

9.5. Poznámka. V úvodní kapitole o Gaussově eliminační metodě jsme vlastně nevědomky vyslovili Frobeniovu větu. V této kapitole jsme si říkali, jak poznáme, že soustava má řešení. Mluvili jsme tam o tom, že soustava nemá řešení právě tehdy, když poslední řádek rozšířené matice soustavy po přímém chodu eliminace je tvaru

$$(0 \quad 0 \quad \cdots \quad 0 \mid c), \quad c \neq 0.$$

Vzpomeneme-li si na metodu počítání hodnosti z příkladu ??, vidíme, že existence takového řádku je ekvivalentní s tím, že rozšířená matice soustavy má o jedničku větší hodnost, než matice soustavy. Uvědomíme si ještě, že hodnost rozšířené matice soustavy může být buď o jedničku větší nebo přímo rovna hodnosti matice soustavy. Žádná jiná možnost pro hodnosti těchto matic neexistuje.

9.6. Definice. Nechť $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ je soustava m lineárních rovnic o n neznámých a $\mathbf{C}\,\boldsymbol{x} = \boldsymbol{d}$ je soustava k lineárních rovnic o stejném počtu n neznámých. Říkáme, že tyto soustavy jsou *ekvivalentní*, pokud obě soustavy mají stejné množiny řešení.

9.7. Poznámka. Gaussova eliminační metoda řešení soustav lineárních rovnic popsaná v úvodní kapitole spočívá v převedení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ na soustavu $\mathbf{C}\,\boldsymbol{x} = \boldsymbol{d}$, která je s původní soustavou rovnic ekvivalentní. Přitom řešení soustavy $\mathbf{C}\,\boldsymbol{x} = \boldsymbol{d}$ lze nalézt snadněji, protože $\mathbf{C}$ je schodovitá matice (srovnejte větu ??). Tuto skutečnost zaznamenáme do následující věty.

9.8. Věta. Ke každé soustavě $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ lze nalézt ekvivalentní soustavu $\mathbf{C}\,\boldsymbol{x} = \boldsymbol{d}$, jejíž matice $\mathbf{C}$ je schodovitá.

Důkaz. Podle věty ?? lze nalézt $(\mathbf{C}|\boldsymbol{d})$ takovou, že $(\mathbf{A}|\boldsymbol{b}) \sim (\mathbf{C}|\boldsymbol{d})$, a přitom $\mathbf{C}$ je schodovitá matice. Protože operace „$\sim$“ zde označuje konečně mnoho elementárních kroků Gaussovy eliminační metody, a protože jsme si řekli v úvodní kapitole, že tyto elementární kroky nemění

množinu řešení odpovídající soustavy, je soustava $\mathbf{C}\,\boldsymbol{x} = \boldsymbol{d}$ ekvivalentní s původní soustavou $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$.

9.9. Definice. Existuje-li v matici $\boldsymbol{b}$ aspoň jeden prvek nenulový, říkáme, že je soustava lineárních rovnic $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ *nehomogenní*. Jsou-li všechny prvky v matici $\boldsymbol{b}$ nulové, nazýváme soustavu rovnic *homogenní* a zapisujeme ji takto:

$$\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o} \qquad \text{(symbolem } \boldsymbol{o} \in \mathbf{R}^{m,1} \text{ zde značíme sloupcový nulový vektor).}$$

9.10. Věta.* Množina všech řešení homogenní soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$ s n neznámými tvoří lineární podprostor lineárního prostoru $\mathbf{R}^n$.

Důkaz. Věta by správně měla znít: množina řešení homogenní soustavy tvoří lineární podprostor lineárního prostoru $\mathbf{R}^{n,1}$, ovšem v souladu s poznámkou ?? nebudeme rozlišovat mezi $\mathbf{R}^{n,1}$ a $\mathbf{R}^n$.

Především množina řešení homogenní soustavy je neprázdná, protože nulový vektor v $\mathbf{R}^{n,1}$ je samozřejmě řešením této soustavy.

Podle definice ?? musíme dále dokázat: (1) jsou-li $\boldsymbol{u} \in \mathbf{R}^{n,1}$ a $\boldsymbol{v} \in \mathbf{R}^{n,1}$ řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$, pak též $\boldsymbol{u}+\boldsymbol{v}$ je řešením stejné soustavy. (2) je-li $\boldsymbol{u} \in \mathbf{R}^{n,1}$ řešením soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$ a $\alpha \in \mathbf{R}$, pak též $\alpha\,\boldsymbol{u}$ je řešením stejné soustavy.

Protože $\boldsymbol{u}$ a $\boldsymbol{v}$ jsou řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$, platí: $\mathbf{A}\,\boldsymbol{u} = \boldsymbol{o}$ a $\mathbf{A}\,\boldsymbol{v} = \boldsymbol{o}$. Máme dokázat, že pak také $\mathbf{A}\,(\boldsymbol{u} + \boldsymbol{v}) = \boldsymbol{o}$ a $\mathbf{A}\,(\alpha\,\boldsymbol{u}) = \boldsymbol{o}$. Podle věty ?? je

$$\mathbf{A}\,(\boldsymbol{u} + \boldsymbol{v}) = \mathbf{A}\,\boldsymbol{u} + \mathbf{A}\,\boldsymbol{v} = \boldsymbol{o} + \boldsymbol{o} = \boldsymbol{o},$$
$$\mathbf{A}\,(\alpha\,\boldsymbol{u}) = \alpha\,\mathbf{A}\,\boldsymbol{u} = \alpha\,\boldsymbol{o} = \boldsymbol{o}.$$

9.11. Příklad. Najdeme množinu všech řešení homogenní soustavy lineárních rovnic se šesti neznámými:

$$\begin{aligned} x_1 + x_2 + 2x_3 + 3x_4 + 3x_5 + 3x_6 &= 0 \\ x_1 + x_2 + x_3 + 3x_4 + x_5 + x_6 &= 0 \\ 2x_1 + 2x_2 + 2x_3 + 6x_4 + 2x_5 + 8x_6 &= 0 \end{aligned}$$

Eliminujeme matici soustavy (vektor pravých stran je nulový, takže je zbytečné jej psát).

$$\begin{pmatrix} 1 & 1 & 2 & 3 & 3 & 3 \\ 1 & 1 & 1 & 3 & 1 & 1 \\ 2 & 2 & 2 & 6 & 2 & 8 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 3 & 3 & 3 \\ 0 & 0 & -1 & 0 & -2 & -2 \\ 0 & 0 & -2 & 0 & -4 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 3 & 3 & 3 \\ 0 & 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 6 \end{pmatrix}.$$

Z poslední rovnice budeme počítat x_6, z předposlední rovnice x_3 a z první rovnice x_1. Hodnoty neznámých x_2, x_4, x_5 mohou být libovolné. Zaveďme pro ně parametry $x_2 = t$, $x_4 = u$, $x_5 = v$. Z poslední rovnice vychází jedině $x_6 = 0$, z předposlední rovnice máme $x_3 = -2v$ a konečně

z první rovnice dostáváme $x_1 = -t + 4v - 3u - 3v = -t + v - 3u$. Výsledek sumarizujeme takto:

$$\begin{aligned}(x_1, x_2, x_3, x_4, x_5, x_6) &= (-t + v - 3u,\ t,\ -2v,\ u,\ v,\ 0) = \\ &= t\,(-1, 1, 0, 0, 0, 0) + u\,(-3, 0, 0, 1, 0, 0) + v\,(1, 0, -2, 0, 1, 0).\end{aligned}$$

Z tohoto zápisu vyplývá, že množina všech řešení dané homogenní soustavy je množinou všech lineárních kombinací uvedených tří vektorů, což můžeme zapsat pomocí lineárního obalu takto:

$$M_0 = \big\langle (-1, 1, 0, 0, 0, 0), (-3, 0, 0, 1, 0, 0), (1, 0, -2, 0, 1, 0) \big\rangle.$$

9.12. Poznámka. Protože uvedené tři vektory z výsledku příkladu ?? jsou lineárně nezávislé, tvoří jednu z možných bází prostoru M_0. To se nestalo náhodou, ale platí to vždy, jak ukazuje následující věta.

9.13. Věta. Nechť $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$ je homogenní soustava lineárních rovnic o n neznámých, $k = n - \operatorname{hod}\mathbf{A}$. Pak existuje k lineárně nezávislých vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ z $\mathbf{R}^n$ takových, že pro množinu M_0 všech řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$ platí

$$M_0 = \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle \quad \text{pro } k > 0, \qquad M_0 = \{\boldsymbol{o}\} \quad \text{pro } k = 0.$$

Vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ tvoří jednu z možných bází lineárního prostoru všech řešení M_0.

Důkaz. Vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ najdeme analogicky, jako jsme to udělali v příkladu ??. Algoritmus ?? zaručuje, že počet rovnic soustavy po eliminaci je roven $\hod \mathbf{A}$ a je roven počtu neznámých, které můžeme z rovnic vypočítat. Ostatních $k = n - \hod \mathbf{A}$ neznámých $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$ může nabývat libovolných hodnot a zaveďme pro ně parametry $x_{i_1} = p_1, x_{i_2} = p_2, \ldots, x_{i_k} = p_k$. Všechna řešení získáme například dosazovací metodou použitou na rovnice po eliminaci (začínáme poslední rovnicí a končíme první). Z tohoto řešení můžeme vytknout parametry:

$$(x_1, x_2, \ldots, x_n) = p_1\,\boldsymbol{u}_1 + p_2\,\boldsymbol{u}_2 + \cdots + p_k\,\boldsymbol{u}_k \tag{9.2}$$

a dostáváme hledané vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$. Z uvedené rovnosti a z definice lineárního obalu ?? přímo plyne, že pro množinu všech řešení platí $M_0 = \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle$.

Zbývá dokázat, že vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ jsou lineárně nezávislé. Označme $\boldsymbol{u}'_1 \in \mathbf{R}^k$, $\boldsymbol{u}'_2 \in \mathbf{R}^k, \ldots, \boldsymbol{u}'_k \in \mathbf{R}^k$ ty části vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$, které obsahují jen složky $i_1, i_2, \ldots, i_k$. Protože platí rovnost (9.2) a také platí označení $x_{i_1} = p_1, x_{i_2} = p_2, \ldots, x_{i_k} = p_k$, dostáváme

$$\boldsymbol{u}'_1 = (1, 0, 0, \ldots, 0), \quad \boldsymbol{u}'_2 = (0, 1, 0, \ldots, 0), \quad \ldots, \quad \boldsymbol{u}'_k = (0, 0, 0, \ldots, 1).$$

Toto jsou lineárně nezávislé vektory. Z toho plyne, že jsou lineárně nezávislé i vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots,$ protože $\boldsymbol{u}'_1, \boldsymbol{u}'_2, \ldots, \boldsymbol{u}'_k$ jsou jejich části.

Závěrečné tvrzení věty, že vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ tvoří bázi prostoru řešení homogenní soustavy, plyne přímo z definice báze ??.

9.14. Věta.* Nechť M_0 je lineární prostor všech řešení homogenní soustavy lineárních rovnic $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$ s n neznámými. Pak $\dim M_0 = n - \operatorname{hod}\mathbf{A}$.

Důkaz. Věta je přímým důsledkem předchozí věty ??.

9.15. Poznámka. Nechť n je počet neznámých homogenní soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$. Pak z věty ?? plyne tento důsledek:

$$\begin{aligned} \operatorname{hod}\mathbf{A} = n &\quad \text{pak soustava má jen nulové řešení,} \\ \operatorname{hod}\mathbf{A} < n &\quad \text{pak soustava má nekonečně mnoho řešení.} \end{aligned}$$

9.16. Definice. Nechť $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ je nehomogenní soustava lineárních rovnic o n neznámých a $\boldsymbol{v} \in \mathbf{R}^n$ je nějaké jedno její řešení. Takovému řešení $\boldsymbol{v}$ říkáme *partikulární řešení* nehomogenní soustavy.

Pokud zaměníme sloupcový vektor $\boldsymbol{b}$ za nulový vektor stejného typu, dostáváme homogenní soustavu $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$, kterou nazýváme *přidruženou homogenní soustavou* k soustavě $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$.

9.17. Věta. (1) Nechť $\boldsymbol{v}$ je partikulární řešení nehomogenní soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ a $\boldsymbol{u}$ je libovolné řešení přidružené homogenní soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$. Pak $\boldsymbol{v} + \boldsymbol{u}$ je také řešením soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$.

(2) Nechť $\boldsymbol{v}$ a $\boldsymbol{w}$ jsou dvě partikulární řešení nehomogenní soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$. Pak $\boldsymbol{v} - \boldsymbol{w}$ je řešením přidružené homogenní soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$.

Důkaz. (1) Podle předpokladu platí $\mathbf{A}\,\boldsymbol{v} = \boldsymbol{b}$, $\mathbf{A}\,\boldsymbol{u} = \boldsymbol{o}$. Pro součet $\boldsymbol{v} + \boldsymbol{u}$ pak platí

$$\mathbf{A}\,(\boldsymbol{v} + \boldsymbol{u}) = \mathbf{A}\,\boldsymbol{v} + \mathbf{A}\,\boldsymbol{u} = \boldsymbol{b} + \boldsymbol{o} = \boldsymbol{b}.$$

(2) Podle předpokladu platí $\mathbf{A}\,\boldsymbol{v} = \boldsymbol{b}$, $\mathbf{A}\,\boldsymbol{w} = \boldsymbol{b}$. Pro rozdíl $\boldsymbol{v} - \boldsymbol{w}$ pak platí

$$\mathbf{A}\,(\boldsymbol{v} - \boldsymbol{w}) = \mathbf{A}\,\boldsymbol{v} - \mathbf{A}\,\boldsymbol{w} = \boldsymbol{b} - \boldsymbol{b} = \boldsymbol{o}.$$

9.18. Věta.* Nechť $\boldsymbol{v}$ je partikulární řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ a M_0 je lineární prostor všech řešení přidružené homogenní soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$. Pak pro množinu M všech řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ platí

$$M = \{\boldsymbol{v} + \boldsymbol{u};\ \ \boldsymbol{u} \in M_0\}.$$

Důkaz. Z vlastnosti (1) věty ?? plyne, že $\{\boldsymbol{v} + \boldsymbol{u};\ \ \boldsymbol{u} \in M_0\} \subseteq M$. Stačí dokázat obrácenou inkluzi. Pokud $\boldsymbol{w} \in M$, pak podle vlastnosti (2) věty ?? existuje $\boldsymbol{u} = \boldsymbol{w} - \boldsymbol{v} \in M_0$, takže $\boldsymbol{w} \in \{\boldsymbol{v} + \boldsymbol{u};\ \ \boldsymbol{u} \in M_0\}$. Platí tedy i obrácenná inkluze.

9.19. Poznámka. Množinu všech řešení nehomogenní soustavy lineárních rovnic zapisujeme většinou zjednodušeně jako součet partikulárního řešení a lineárního prostoru všech řešení přidružené homogenní soustavy takto:

$$M = \boldsymbol{v} + M_0 = \boldsymbol{v} + \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle. \tag{9.3}$$

Řešit nehomogenní soustavu tedy znamená najít partikulární řešení $\boldsymbol{v}$ a dále najít k lineárně nezávislých řešení přidružené homogenní soustavy $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ (k je rovno počtu neznámých mínus hodnost matice soustavy). Výsledek je obvyklé psát ve tvaru (9.3).

9.20. Příklad. Najdeme množinu všech řešení soustavy lineárních rovnic se šesti neznámými:

$$\begin{aligned} x_1 + x_2 + 2x_3 + 3x_4 + 3x_5 + 3x_6 &= 1 \\ x_1 + x_2 + x_3 + 3x_4 + x_5 + x_6 &= -1 \\ 2x_1 + 2x_2 + 2x_3 + 6x_4 + 2x_5 + 8x_6 &= 10 \end{aligned}$$

Eliminujeme rozšířenou matici soustavy.

$$\left(\begin{array}{cccccc|c} 1 & 1 & 2 & 3 & 3 & 3 & 1 \\ 1 & 1 & 1 & 3 & 1 & 1 & -1 \\ 2 & 2 & 2 & 6 & 2 & 8 & 10 \end{array}\right) \sim \left(\begin{array}{cccccc|c} 1 & 1 & 2 & 3 & 3 & 3 & 1 \\ 0 & 0 & -1 & 0 & -2 & -2 & -2 \\ 0 & 0 & -2 & 0 & -4 & 2 & 8 \end{array}\right) \sim \left(\begin{array}{cccccc|c} 1 & 1 & 2 & 3 & 3 & 3 & 1 \\ 0 & 0 & 1 & 0 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 6 & 12 \end{array}\right) \sim \left(\begin{array}{cccccc} 1 & 1 & 2 & 3 & 3 & \\ 0 & 0 & 1 & 0 & 2 & \\ 0 & 0 & 0 & 0 & 0 & \end{array}\right.$$

Z poslední rovnice budeme počítat x_6, z předposlední rovnice x_3 a z první rovnice x_1. Hodnoty neznámých x_2, x_4, x_5 mohou být libovolné. Zaveďme pro ně parametry $x_2 = t$, $x_4 = u$, $x_5 = v$.

Z poslední rovnice máme $x_6 = 2$, z předposlední rovnice $x_3 = 2 - 2v - 2 \cdot 2 = -2 - 2v$ a konečně z první rovnice dostáváme $x_1 = 1 - t - 2(-2 - 2v) - 3u - 3v - 3 \cdot 2 = -1 - t + v - 3u$. Výsledek sumarizujeme takto:

$$\begin{aligned}(x_1, x_2, x_3, x_4, x_5, x_6) &= (-1 - t + v - 3u, t, -2 - 2v, u, v, 2) = \\ &= (-1, 0, -2, 0, 0, 2) + t\,(-1, 1, 0, 0, 0, 0) + u\,(-3, 0, 0, 1, 0, 0) + v\,(1, 0, -2,\end{aligned}$$

Z tohoto zápisu vyplývá, že množina všech řešení dané nehomogenní soustavy je rovna

$$M = (-1, 0, -2, 0, 0, 2) + \big\langle (-1, 1, 0, 0, 0, 0), (-3, 0, 0, 1, 0, 0), (1, 0, -2, 0, 1, 0) \big\rangle.$$

Vektor $(-1, 0, -2, 0, 0, 2)$ je partikulárním řešením dané nehomogenní soustavy a vektory $(-1, 1, 0, 0, 0, 0)$, $(-3, 0, 0, 1, 0, 0)$, $(1, 0, -2, 0, 1, 0)$ tvoří bázi prostoru řešení přidružené homogenní soustavy.

9.21. Poznámka. Ve výše uvedeném příkladě jsem spočítali partikulární řešení i bázi množiny řešení přidružené homogenní soustavy v jediném postupu. Často ale takovéto lineární úlohy řešíme ve dvou krocích. Nejprve najdeme bázi řešení přidružené homogení soustavy

(to jsme provedli v příkladu ??) a poté je třeba „uhodnout“ jedno řešení dané nehomogení soustavy. Takové řešení prohlásíme za partikulární řešení. Nakonec zapíšeme výsledek v souladu s poznámkou ?? ve formě „partikulární řešení plus lineární obal báze množiny řešení přidružené homogenní soustavy“.

Partikulární řešení můžeme najít po přímém chodu eliminační metody, když rozhodneme, které proměné budeme pomocí rovnic počítat. Těm ostatním proměným můžeme přidělit jakákoli čísla, třeba nuly. Po dosazení těchto čísel vzniká soustava, která má stejně rovnic jako neznámých a má regulární matici, tedy má jediné řešení. Toto řešení obsahuje hodnoty hledaných proměnných.

Třeba v příkladě ?? jsme rozhodli, že budeme počítat proměnné x_1, x_3, x_6, takže při hledání partikulárního řešení proměnným x_2, x_4, x_5 přidělíme třeba nuly. Po dosazení těchto nul dostáváme soustavu s maticí

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

Nyní můžeme použít zpětný chod Gaussovy eliminační metody nebo počítat dosazovací metodou od poslední rovnice k první. Dostáváme řešení $x_1 = -1, x_3 = -2, x_6 = 2$, takže partikulárním řešením je $(-1, 0, -2, 0, 0, 2)$.

9.22. Poznámka. Při strojovém hledání řešení rozsáhlých soustav většinou jde o to najít jedno partikulární řešení a bázi prostoru řešení přidružené homogenní soustavy. Přitom

není nutné programovat symbolické výpočty, jako je například vytýkání parametrů podle rovnosti (9.2). V následujícím textu ukážeme, že stačí využít Gaussovu eliminační metodu.

K nalezení báze přidružené homogenní soustavy můžeme použít následující větu ?? a k nalezení partikulírního řešení využijeme větu ??.

9.23. Věta. Nechť homogenní soustava lineárních rovnic $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$ má matici soustavy ve tvaru

$$\mathbf{A} = (\mathbf{E} \,|\, \mathbf{C}),$$

kde $\mathbf{E} \in \mathbf{R}^{m,m}$ je jednotková matice a $\mathbf{C} \in \mathbf{R}^{m,k}$ je libovolná matice. Pak existuje báze řešení této soustavy $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$, která má tvar:

$$\begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \\ \vdots \\ \boldsymbol{b}_k \end{pmatrix} = (-\mathbf{C}^T \,|\, \mathbf{E}'),$$

kde $\mathbf{E}' \in \mathbf{R}^{k,k}$ je jednotková matice.

Důkaz. Nejprve překontrolujeme rozměry matic. Nechť počet neznámých soustavy je n, takže matice soustavy $\mathbf{A}$ je typu (m, n). Počet sloupců n této matice se skládá z m sloupců (matice

$\mathbf{E}$) a k sloupců (matice $\mathbf{C}$). Je tedy $n = m+k$. Dimenze prostoru řešení je podle věty ?? rovna počtu neznámých minus hod $\mathbf{A}$, což je $n - m = k$. To sedí. Skutečně matice $\mathbf{B} = (-\mathbf{C}^T|\mathbf{E}')$ má k řádků a tyto jsou lineárně nezávislé (díky matici $\mathbf{E}'$). Matice $\mathbf{B}$ tedy může obsahovat řádky báze prostoru řešení. Stačí jen ověřit, že každý řádek matice $\mathbf{B}$ řeší soustavu $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$. Tj. stačí ověřit, že $\mathbf{A} \cdot \mathbf{B}^T = \mathbf{O}$, kde $\mathbf{O}$ je nulová matice typu (m, k):

$$\mathbf{A} \cdot \mathbf{B}^T = (\mathbf{E} \,|\, \mathbf{C}) \cdot \begin{pmatrix} -\mathbf{C} \\ \hline \mathbf{E}' \end{pmatrix} = \mathbf{E} \cdot (-\mathbf{C}) + \mathbf{C} \cdot \mathbf{E}' = -\mathbf{C} + \mathbf{C} = \mathbf{O}.$$

9.24. Poznámka. Tato věta nám umožňuje rovnou napsat bázi řešení homogenní soustavy, pokud je matice soustavy v uvedeném tvaru. Dokonce, pokud matice soustavy není v uvedeném tvaru, je někdy možné jí eliminací do tohoto tvaru převést, tj. ekvivalentní soustava může mít tento tvar. Pokud ani ekvivalentní soustava nemá tento tvar, dá se prohozením pořadí neznámých dospět k požadovanému tvaru matice soustavy. V takovém případě je ovšem nutné před zapsáním báze prostoru řešení prohodit sloupce matice $\mathbf{B} = (-\mathbf{C}^T|\mathbf{E}')$ zpět. Místo dlouhého vysvětlování ukážeme použití věty na našem příkladu ??.

9.25. Příklad. Najdeme bázi prostoru řešení soustavy z příkladu ??. Eliminujeme matici soustavy:

$$\begin{pmatrix} 1 & 1 & 2 & 3 & 3 & 3 \\ 1 & 1 & 1 & 3 & 1 & 1 \\ 2 & 2 & 2 & 6 & 2 & 8 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 3 & 3 & 3 \\ 0 & 0 & -1 & 0 & -2 & -2 \\ 0 & 0 & -2 & 0 & -4 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 3 & 3 & 3 \\ 0 & 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 3 & 3 & 3 \\ 0 & 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Eliminujeme dále zpětným chodem, abychom ve sloupcích 1, 3 a 6 dostali jednotkové vektory:

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

Prohodíme druhý sloupec s třetím a poslední sloupec s novým třetím (měníme pořadí proměnných)

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

a dostáváme matici podle předpokladu věty ??. Bázi řešení soustavy s takovou maticí můžeme podle této věty zapsat do matice, kde každý řádek obsahuje jeden vektor báze:

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

Zpětně přehodíme poslední sloupec s třetím a druhý s novým třetím a dostáváme matici, obsahující (po řádcích) bázi řešení původní soustavy

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

9.26. Věta. Nechť soustava lineárních rovnic $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ má matici soustavy ve tvaru

$$\mathbf{A} = (\mathbf{E} \,|\, \mathbf{C}),$$

kde $\mathbf{E} \in \mathbf{R}^{m,m}$ je jednotková matice a $\mathbf{C} \in \mathbf{R}^{m,k}$ je libovolná matice. Pak partikulárním řešením soustavy je vektor $\boldsymbol{v} = (\boldsymbol{b}^T, \boldsymbol{o})$, kde $\boldsymbol{o} \in \mathbf{R}^k$ je nulový vektor.

Důkaz. Stačí dosadit:

$$\mathbf{A} \cdot \begin{pmatrix} \boldsymbol{b} \\ \boldsymbol{o} \end{pmatrix} = (\mathbf{E} \,|\, \mathbf{C}) \begin{pmatrix} \boldsymbol{b} \\ \boldsymbol{o} \end{pmatrix} = \mathbf{E}\boldsymbol{b} + \mathbf{C}\boldsymbol{o} = \boldsymbol{b}.$$

9.27. Příklad. V tomto příkladě si ukážeme „strojové“ řešení soustav lineárních rovnic s využitím vět ?? a ??. K řešení nepotřebujeme nic jiného než dobře namazaný stroj zvládající přímý a zpětný chod Gaussovy eliminační metody.

Najdeme množinu řešení soustavy lineárních rovnic s rozšířenou maticí:

$$\left(\begin{array}{rrrrr|r} 1 & 1 & -1 & 11 & 1 & 3 \\ 1 & 2 & 2 & 8 & 2 & 5 \\ 2 & 5 & 7 & 17 & 6 & 18 \\ 3 & 6 & 6 & 28 & 7 & 21 \end{array}\right)$$

Pomocí přímého chodu eliminační metody matici převedeme na schodovitou matici. Po prohození třetího sloupce s posledním pak dostáváme matici, na které můžeme použít zpětný chod Gaussovy eliminační metody tak, že v levém bloku dostaneme jednotkovou matici. Nad matici jsme si poznamenali změněné pořadí proměných.

$$\left(\begin{array}{ccccc|c} 1 & 1 & -1 & 11 & 1 & 3 \\ 1 & 2 & 2 & 8 & 2 & 5 \\ 2 & 5 & 7 & 17 & 6 & 18 \\ 3 & 6 & 6 & 28 & 7 & 21 \end{array}\right) \sim \begin{array}{c} \begin{array}{ccccc} x_1 & x_2 & x_3 & x_4 & x_5 \end{array} \\ \left(\begin{array}{ccccc|c} 1 & 1 & -1 & 11 & 1 & 3 \\ 0 & 1 & 3 & -3 & 1 & 2 \\ 0 & 0 & 0 & 4 & 1 & 6 \end{array}\right) \end{array} \leftrightarrow \begin{array}{c} \begin{array}{ccccc} x_1 & x_2 & x_5 & x_4 & x_3 \end{array} \\ \left(\begin{array}{ccccc|c} 1 & 1 & 1 & 11 & -1 & 3 \\ 0 & 1 & 1 & -3 & 3 & 2 \\ 0 & 0 & 1 & 4 & 0 & 6 \end{array}\right) \end{array} \sim \left(\begin{array}{ccccc} 1 & 0 & 0 & 14 & - \\ 0 & 1 & 0 & -7 & \\ 0 & 0 & 1 & 4 & \end{array}\right.$$

Podle věty ?? má tato soustava bázi řešení přidružené homogení soustavy zapsanou v řádcích matice:

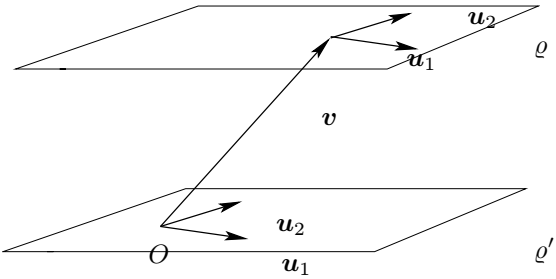
$$(-\mathbf{C}^T \mid \mathbf{E}') = \begin{pmatrix} -14 & 7 & -4 & 1 & 0 \\ 4 & -3 & 0 & 0 & 1 \end{pmatrix}$$

a podle věty ?? je partikulární řešení ve tvaru $(1, -4, 6, 0, 0)$. Po zpětném přehození sloupců tak, abychom popsali výsledek pro neznámé v pořadí $(x_1, x_2, x_3, x_4, x_5)$ dostáváme řešení:

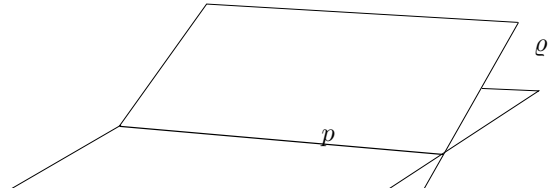
$$(1, -4, 0, 0, 6) + \langle (-14, 7, 0, 1, -4),\ (4, -3, 1, 0, 0) \rangle,$$

které jsme zapsali jako součet partikulárního řešení a lineárního obalu báze množiny řešení přidružené homogenní soustavy, tedy v souladu s poznámkou ??.

9.28. Poznámka. Představme si soustavu lineárních rovnic se třemi neznámými a s jedinou nenulovou rovnicí. Pokud interpretujeme každou uspořádanou trojici, která je řešením soustavy, jako souřadnice bodu v geometrickém prostoru, pak množina všech těchto bodů vyplní rovinu. V případě, že je naše soustava homogenní, pak množina řešení tvoří lineární podprostor dimenze $3 - 1 = 2$, tj. vyplní rovinu ϱ' procházející počátkem O, tj. bodem se souřadnicemi $(0, 0, 0)$. V případě, že soutava má nenulovou pravou stranu, pak množinou řešení je rovina, která neprochází počátkem. Je to rovina ϱ rovnoběžná s množinou řešení přidružené homogenní soustavy ϱ' a prochází bodem, který je dán jako partikulární řešení $\boldsymbol{v}$. Viz obrázek.



9.29. Poznámka. Představme si soustavu dvou lineárně nezávislých lineárních rovnic o třech neznámých. Množinu řešení interpretujme jako body v prostoru stejně jako v předchozí poznámce. Řešení první rovnice vy-



plní rovinu ϱ a řešení druhé rovnice vyplní rovinu σ (viz obrázek). Takže řešení obou rovnic „společně“ je průnikem rovin ϱ a σ. To je přímka, označme ji p. Dimenze množiny řešení přidružené homogenní soustavy je podle věty ?? rovna $3 - 2 = 1$.

9.30. Poznámka. Tři lineárně nezávislé rovnice o třech neznámých mají jednobodové řešení, které je průnikem tří rovin, kde každá rovina je množinou řešení jedné rovnice.

9.31. Poznámka. Nemá-li soustava tří rovnic o třech neznámých řešení, pak jednotlivé rovnice mají jako své množiny řešení roviny, které nemají společný průnik. Uvědomíme si, jakým způsobem se to může stát: buď jsou dvě roviny rovnoběžné a nikoli totožné, nebo mají roviny jako průnik přímky, které jsou rovnoběžné.

9.32. Poznámka.* Má-li soustava lineárních rovnic n neznámých, pak množinou řešení je podmnožina $\mathbf{R}^n$. Představme si, že nyní $n > 3$. S trochou fantazie je možné si i tyto podmnožiny představit geometricky jako *zobecněné roviny*.

Pojem *zobecněná rovina* se používá pro analogický geometrický útvar jako je rovina nebo přímka v geometrickém prostoru, ale může mít libovolnou (třeba větší) dimenzi. Zobecněná rovina nemusí na rozdíl od lineárního podprostoru procházet počátkem. Pokud ji ale posuneme

do počátku, tvoří podprostor. Mluvíme-li tedy o *dimenzi zobecněné roviny*, máme na mysli dimenzi lineárního podprostoru, který vznikne posunutím zkoumané zobecněné roviny tak, aby procházela počátkem.

Množina řešení jedné rovnice ze soustavy je zobecněná rovina, která má dimenzi $n-1$. Množina řešení celé soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ je průnikem těchto zobecněných rovin a je to zase zobecněná rovina ϱ, která má podle věty ?? dimenzi $n - \operatorname{hod}\mathbf{A}$. Množina řešení přidružené homogenní soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$ je zobecněná rovina ϱ' taková, že prochází počátkem a $\varrho = \boldsymbol{v} + \varrho'$, kde $\boldsymbol{v}$ je partikulární řešení. Tedy ϱ vzniká z ϱ' posunutím o $\boldsymbol{v}$. Nebo obráceně, ϱ' vzniká posunutím ϱ o vektor $-\boldsymbol{v}$.

Obrázky u poznámek ?? a ?? lze využít jako ilustraci pro množiny řešení libovolné soustavy lineárních rovnic. První obrázek říká, že zobecněná rovina, která je množinou řešení nehomogenní soustavy lineárních rovnic, je posunutá z počátku o partikulární řešení. Druhý obrázek říká, že množina řešení je zobecněná rovina, která je průnikem nadrovin, které jsou řešeními jednotlivých rovnic.

9.33. Poznámka. Řešení soustavy jako průnik řešení jednotlivých rovnic, jak je popsáno v předchozích poznámkách, je pohled na řešení po rozdělení rozšířené matice soustavy $(\mathbf{A} \mid \boldsymbol{b})$ na jednotlivé řádky. Každý řádek odpovídá jedné rovnici. Někdy se hodí jiný, sloupcový pohled, na řešení sousavy. Rozepišme matici soustavy na sloupce $\mathbf{A} = (\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$. Pak maticové

násobení ve výrazu $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ můžeme přepsat takto:

$$\mathbf{A} \cdot \mathbf{x} \;=\; (\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n) \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \;=\; x_1\mathbf{A}_1 + x_2\mathbf{A}_2 + \cdots + x_n\mathbf{A}_n \;=\; \mathbf{b}$$

takže řešení obsahuje koeficienty takové lineární kombinace sloupců, která je rovna vektoru pravých stran $\boldsymbol{b}$.

9.34. Poznámka. Již v úvodní kapitole o Gaussově eliminační metodě jsme zmínili, že množinu řešení soustavy lineárních rovnic neumíme popsat jednoznačným způsobem. Výjimkou je pouze případ, kdy má soustava jediné řešení. Víme totiž, že každý netriviální lineární podprostor má nekonečně mnoho bází a má-li soustava více řešení, pak i partikulární řešení může každý řešitel zapsat jiné.

K různým zápisům téže množiny řešení můžeme dospět při výpočtu třeba tak, že volíme rozdílnou skupinu neznámých, které mohou nabývat libovolných hodnot. I při stejné skupině těchto neznámých nás nikdo nenutí, abychom tyto neznámé položili rovny jednonásobku parametru. V modelových řešeních příkladů ze skript se můžeme setkat někdy i s jinak volenými parametry tak, aby výsledek vyšel bez použití zlomků pouze s malými celými čísly. Tuto dovednost nebudeme v praktických příkladech (které nejsou modelové) potřebovat, takže nás

nemusí frustrovat, že nám vycházejí ve výsledcích zlomky. Můžeme ovšem v závěru výpočtu každý vektor báze vynásobit společným jmenovatelem všech zlomků v jednotlivých složkách a znovu dostáváme vektory báze stejného lineárního prostoru, tentokrát s celočíselnými složkami.

Kvůli nejednoznačnosti popisu řešení soustav lineárních rovnic je užitečné vědět, jak poznáme, že dva různé popisy řešení popisují stejnou množinu řešení. To je rozebráno podrobně v následující poznámce.

9.35. Poznámka.* Co uděláme, pokud se nám dostanou do ruky dva zápisy řešení nějaké soustavy lineárních rovnic, a přitom nemáme k dispozici původní soustavu a nemůžeme tedy dosazovat? Jak v tomto případě poznáme, že oba zápisy popisují stejné řešení? Jsou dány třeba tyto zápisy:

$$\boldsymbol{v} + \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle \stackrel{?}{=} \boldsymbol{w} + \langle \boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_k \rangle$$

Nejprve ověříme lineární nezávislost vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ a lineární nezávislost vektorů $\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_k$. Dále zjistíme algoritmem ??, zda jsou rovny lineární obaly. Nakonec zjistíme, zda obě partikulární řešení popisují stejnou množinu řešení třeba podle vlastnosti (2) věty ?? tímto testem: $\boldsymbol{v} - \boldsymbol{w} \in \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle$. Na to se hodí algoritmus ??.

Spojením obou algoritmů dostáváme následující test: uvedené množiny se rovnají právě tehdy když vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ jsou lineárně

$$\mathsf{C} = \begin{pmatrix} \boldsymbol{u}_1 \\ \boldsymbol{u}_2 \\ \vdots \\ \boldsymbol{u}_k \\ \boldsymbol{g}_1 \\ \boldsymbol{g}_2 \\ \vdots \end{pmatrix}$$

nezávislé i vektory $\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_k$ jsou lineárně nezávislé a hodnost matice $\mathbf{C}$ (zapsaná zde vpravo) je rovna k. Protože pro velká k je matice $\mathbf{C}$ „příliš vysoká“, je někdy výhodné místo toho počítat hodnost matice $\mathbf{C}^T$. Podle věty ?? dostaneme stejný výsledek, ale navíc šetříme papírem a dalšími kancelářskými technologiemi.

9.36. Příklad. Prověříme, zda množina

$$M_1 = (1,2,-4,-1,1,2) + \big\langle (7,1,-4,-2,2,0), (-8,3,-2,2,1,0), (2,-2,-6,1,3,0) \big\rangle$$

je rovna množině M z příkladu ??.

Díky tomu, že naše řešení z příkladu ?? obsahuje na pozicích 2, 4 a 5 systematicky rozmístěné nuly a jedničky, můžeme okamžitě pohledem do těchto pozic psát následující koeficienty lineárních kombinací:

$$\begin{aligned}
(7,1,-4,-2,2,0) &= 1\,(-1,1,0,0,0,0) - 2\,(-3,0,0,1,0,0) + 2\,(1,0,-2,0,1,0),\\
(-8,3,-2,2,1,0) &= 3\,(-1,1,0,0,0,0) + 2\,(-3,0,0,1,0,0) + 1\,(1,0,-2,0,1,0),\\
(2,-2,-6,1,3,0) &= -2\,(-1,1,0,0,0,0) + 1\,(-3,0,0,1,0,0) + 3\,(1,0,-2,0,1,0),\\
(1,2,-4,-1,1,2) &= (-1,0,-2,0,0,2) + 2\,(-1,1,0,0,0,0) - 1\,(-3,0,0,1,0,0) + 1\,(1,0,-2,0,1
\end{aligned}$$

Tyto rovnosti platí i v ostatních složkách (nejen ve složkách 2, 4 a 5) a můžeme tedy prohlásit, že $M_1 = M$.

Pro porovnání zkusíme ještě metodu počítání hodnosti matice $\mathbf{C}$ z poznámky ??. Nejprve musíme ověřit, zda jsou vektory $(7,1,-4,-2,2,0), (-8,3,-2,2,1,0), (2,-2,-6,1,3,0)$ lineárně nezávislé (například eliminací třířádkové matice obsahující tyto vektory). Zjistíme, že jsou lineárně nezávislé. Pak spočítáme hodnost matice $\mathbf{C}$:

$$\mathbf{C}^T = \begin{pmatrix} -1 & -3 & 1 & 7 & -8 & 2 & -2 \\ 1 & 0 & 0 & 1 & 3 & -2 & -2 \\ 0 & 0 & -2 & -4 & -2 & -6 & 2 \\ 0 & 1 & 0 & -2 & 2 & 1 & 1 \\ 0 & 0 & 1 & 2 & 1 & 3 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} -1 & -3 & 1 & 7 & -8 & 2 & -2 \\ 0 & -3 & 1 & 8 & -5 & 0 & -4 \\ 0 & 1 & 0 & -2 & 2 & 1 & 1 \\ 0 & 0 & -2 & -4 & -2 & -6 & 2 \\ 0 & 0 & 1 & 2 & 1 & 3 & -1 \end{pmatrix} \sim \begin{pmatrix} -1 & -3 & 1 & 7 & -8 & 2 \\ 0 & -3 & 1 & 8 & -5 & 0 \\ 0 & 0 & 1 & 2 & 1 & 3 \end{pmatrix}$$

Je $\operatorname{hod} \mathbf{C} = 3$, takže platí $M = M_1$.

9.37. Poznámka. Je-li $\mathbf{A}$ čtvercová matice, pak je výhodné při řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ spočítat $\det \mathbf{A}$.

Pro $\det \mathbf{A} \neq 0$ je $\operatorname{hod} \mathbf{A}$ rovna počtu neznámých, tj. matice $\mathbf{A}$ je regulární a soustava má jediné řešení. Množina řešení přidružené homogenní soustavy obsahuje totiž v tomto případě jediné řešení: nulový vektor. Po vynásobení rovnosti $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ inverzní maticí $\mathbf{A}^{-1}$ zleva máme okamžitě řešení soustavy $\boldsymbol{x} = \mathbf{A}^{-1}\,\boldsymbol{b}$. Navíc můžeme použít pro zjištění jednotlivých složek řešení tzv. Cramerovo pravidlo (viz následující větu).

Pro $\det \mathbf{A} = 0$ je $\operatorname{hod} \mathbf{A}$ menší než počet neznámých. Pokud má tato soustava podle Frobeniovy věty ?? řešení, pak po eliminaci a odstranění nulových řádků dostáváme soustavu, která už nemá čtvercovou matici. V tomto případě nezbývá nic jiného, než použít postup pro nalezení všech řešení, který byl již vyložen dříve.

9.38. Věta (Cramerovo pravidlo).* Nechť $\mathbf{A}$ je regulární čtvercová matice. Pak pro i-tou složku řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ platí

$$\alpha_i = \frac{\det \mathbf{B}_i}{\det \mathbf{A}}\,,$$

kde matice $\mathbf{B}_i$ je shodná s maticí $\mathbf{A}$ až na i-tý sloupec, který je zaměněn za sloupec pravých stran.

Důkaz. Víme, že platí $\boldsymbol{x} = \mathbf{A}^{-1}\,\boldsymbol{b}$. Podle věty ?? platí

$$\mathbf{A}^{-1} = (c_{i,j}) = \left(\frac{D_{j,i}}{\det \mathbf{A}}\right), \quad \text{kde } D_{i,j} \text{ je matice doplňků k matici } \mathbf{A}.$$

Nechť b_i jsou složky sloupce $\boldsymbol{b}$. Podle definice maticového násobení je

$$\alpha_i = \sum_{j=1}^{n} c_{i,j}\, b_j = \sum_{j=1}^{n} \frac{D_{j,i}}{\det \mathbf{A}}\, b_j = \frac{1}{\det \mathbf{A}} \left(D_{1,i}\, b_1 + D_{2,i}\, b_2 + \cdots + D_{k,i}\, b_k\right) = \frac{\det \mathbf{B}_i}{\det \mathbf{A}}.$$

V poslední rovnosti jsme využili větu o rozvoji determinantu matice $\mathbf{B}_i$ podle i-tého sloupce, viz poznámku ??.

9.39. Příklad. Při řešení soustavy

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 5 \\ 5 & 6 & 8 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 10 \\ 11 \\ 12 \end{pmatrix}$$

použijeme Cramerovo pravidlo. Dostáváme:

$$x_1 = \frac{1}{D}\begin{vmatrix} 10 & 2 & 3 \\ 11 & 4 & 5 \\ 12 & 6 & 8 \end{vmatrix}, \quad x_2 = \frac{1}{D}\begin{vmatrix} 1 & 10 & 3 \\ 3 & 11 & 5 \\ 5 & 12 & 8 \end{vmatrix}, \quad x_3 = \frac{1}{D}\begin{vmatrix} 1 & 2 & 10 \\ 3 & 4 & 11 \\ 5 & 6 & 12 \end{vmatrix}, \quad \text{kde } D = \begin{vmatrix} 1 & 2 & 3 \\ 3 & 4 & 5 \\ 5 & 6 & 8 \end{vmatrix}.$$

Vypočítáním čtyř determinantů z uvedených matic typu (3,3) dostáváme výsledek

$$x_1 = \frac{18}{-2} = -9, \quad x_2 = \frac{-19}{-2} = \frac{19}{2}, \quad x_3 = \frac{0}{-2} = 0, \quad (x_1, x_2, x_3) = \left(-9, \frac{19}{2}, 0\right).$$

9.40. Poznámka. Cramerovo pravidlo se nejeví pro výpočet řešení soustavy s regulární maticí příliš účelné. Potřebujeme spočítat $n+1$ determinantů matic typu (n, n), což je pro velká n náročnější, než spočítat inverzní matici eliminační metodou. Výhodná může být tato metoda pouze tehdy, když nepotřebujeme znát všechny složky řešení, ale jen některé. Například můžeme mít nějaký fyzikální model vyjádřený rozsáhlou soustavou lineárních rovnic, přičemž z mnoha stovek výstupních veličin (tj. složek řešení) nás zajímá jen pár.

9.41. Příklad. Budeme řešit soustavu lineárních rovnic

$$\begin{aligned} x + py + z &= 1 \\ x + 2y + z &= -1 \\ y + pz &= -1 \end{aligned}$$

Rozlišíme různé množiny řešení této soustavy podle hodnot reálného parametru p.

Determinant matice soustavy je roven $D = p\,(2-p)$, takže pro $p \neq 0$ a $p \neq 2$ je matice soustavy regulární a soustava má jediné řešení. Například Cramerovým pravidlem zjistíme toto řešení:

$$x = \frac{1}{D}\begin{vmatrix} 1 & p & 1 \\ -1 & 2 & 1 \\ -1 & 1 & p \end{vmatrix} = \frac{p+1}{2-p}, \quad y = \frac{1}{D}\begin{vmatrix} 1 & 1 & 1 \\ 1 & -2 & 0 \\ 0 & -1 & p \end{vmatrix} = \frac{2}{p-2}, \quad z = \frac{1}{D}\begin{vmatrix} 1 & p & 1 \\ 1 & 2 & -1 \\ 0 & 1 & -1 \end{vmatrix} = \frac{1}{2-p}.$$

Pro $p = 0$ a $p = 2$ musíme řešit soustavu individuálně.

$p = 0$: $\left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 1 & 2 & 1 & -1 \\ 0 & 1 & 0 & -1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & -1 \end{array}\right)$, při $z = t$, vychází $y = -1$, $x = 1 - t$, tj. $(x, y, z) = (1-t, -1, t) = (1, -1, 0) + t(-1, 0, 1)$

množina řešení: $M = (1, -1, 0) + \langle (-1, 0, 1) \rangle$.

$p = 2$: $\left(\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ 1 & 2 & 1 & -1 \\ 0 & 1 & 2 & -1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & -1 \end{array}\right)$, podle Frobeniovy věty soustava pro $p = 2$ nemá

9.42. Poznámka. Seznámíme se s možnostmi řešení většího množství soustav lineárních rovnic se stejnou maticí soustavy, ale s různými pravými stranami. Máme tedy dánu následující „soustavu soustav“ lineárních rovnic:

$$\mathbf{A} \cdot \boldsymbol{x}_1 = \boldsymbol{b}_1, \quad \mathbf{A} \cdot \boldsymbol{x}_2 = \boldsymbol{b}_2, \quad \ldots, \quad \mathbf{A} \cdot \boldsymbol{x}_k = \boldsymbol{b}_k.$$

Matice soustavy $\mathbf{A} \in \mathbf{R}^{m,n}$ je společná všem soustavám. Podle věty ?? vidíme, že uvedená soustava soustav je ekvivalentní maticové rovnici

$$\mathbf{A} \cdot \mathbf{X} = \mathbf{B}$$

kde matice $\mathbf{X} = (\boldsymbol{x}_1\ \boldsymbol{x}_2\ \ldots\ \boldsymbol{x}_k)$ obsahuje vedle sebe napsané sloupcové vektory neznámých z jednotlivých soustav a matice $\mathbf{B} = (\boldsymbol{b}_1\ \boldsymbol{b}_2\ \ldots \boldsymbol{b}_k)$ obsahuje sloupcové vektory pavých stran.

Vyřešit tuto soustavu soustav znamená najít podmnožiny z $\mathbf{R}^n$, které jsou množinami řešení jednotlivých soustav. Tyto množiny řešení jsou tvaru $\boldsymbol{v}_i + M_0$, $i \in \{1, 2, \ldots, k\}$, kde $\boldsymbol{v}_i$ je partikulární i-té soustavy a M_0 je množina řešení přidružené homogenní soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$. Ta je společná všem soustavám.

Při řešení takových soustav soustav je přirozené před zahájením eliminace zapsat všechny sloupce pravých stran vedle sebe a eliminovat společně celou matici. To ilustruje následující příklad.

9.43. Příklad. Řešme maticovou rovnost

$$\begin{pmatrix} 1 & 1 & 2 & 3 & 3 & 3 \\ 1 & 1 & 1 & 3 & 1 & 1 \\ 2 & 2 & 2 & 6 & 2 & 8 \end{pmatrix} \cdot \mathbf{X} = \begin{pmatrix} 2 & 4 & 3 & 3 \\ 2 & 2 & 1 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

Soustavu soustav řešíme eliminací:

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

Přidruženou homogenní soustavu známe už z předchozích příkladů, takže víme, že její prostor řešení má bázi $\{(-1,1,0,0,0,0),(-3,0,0,1,0,0),(1,0,-2,0,1,0)\}$. Partikulární řešení budeme hledat pro každý sloupec pravých stran zvlášť. Počítat budeme poslední, třetí a první složku, v ostatních předpokládáme nuly. Pro sloupec $(2,0,-3)^T$ máme řešení $(\frac{3}{2},0,1,0,0,-\frac{1}{2})$, pro sloupec $(4,2,-2)^T$ máme řešení $(-\frac{1}{3},0,\frac{8}{3},0,0,-\frac{1}{3})$, pro sloupec $(3,2,1)^T$ máme řešení $(-\frac{5}{6},0,\frac{5}{3},0,0,\frac{1}{6})$ a konečně pro sloupec $(3,0,-2)^T$ máme řešení $(\frac{8}{3},0,\frac{2}{3},0,0,-\frac{1}{3})$. Zapíšeme-li tato řešení do sloupců vedle sebe, máme jedno z možných řešení pro hledanou matici $\mathbf{X}$. Když k této matici přičteme matici, která bude mít čtyři stejné sloupce tvaru $\alpha\,(-1,1,0,0,0,0)^T + \beta\,(-3,0,0,1,0,0)^T + \gamma\,(1,0,-2,0,1,0)^T$, $\alpha,\beta,\gamma \in \mathbf{R}$, dostáváme zápis obecně všech matic $\mathbf{X}$, které vyhovují zadané maticové rovnici.

9.44. Poznámka. Maticovou rovnici $\mathbf{XA} = \mathbf{B}$ (při daných maticích $\mathbf{A}$, $\mathbf{B}$) bychom řešili například tak, že transponujeme obě strany rovnosti. Tím dostáváme $\mathbf{A}^T \cdot \mathbf{X}^T = \mathbf{B}^T$ a problém je převeden na tvar, se kterým už si víme rady.

9.45. Věta. Nechť $\mathbf{A}$ je regulární matice a $\mathbf{B}$ je libovolná matice se stejným počtem řádků. Platí:
(1) Maticová rovnost $\mathbf{AX} = \mathbf{B}$ má jediné řešení a tím řešením je $\mathbf{X} = \mathbf{A}^{-1}\,\mathbf{B}$,
(2) Je-li $(\mathbf{A}\,|\,\mathbf{B}) \sim (\mathbf{E}\,|\,\mathbf{C})$, kde $\mathbf{E}$ je jednotková matice, pak $\mathbf{C} = \mathbf{A}^{-1}\,\mathbf{B}$. Neboli $(\mathbf{A}\,|\,\mathbf{B}) \sim (\mathbf{E}\,|\,\mathbf{A}^{-1}\,\mathbf{B})$.

Důkaz. (1) Stačí rovnost $\mathbf{AX} = \mathbf{B}$ vynásobit zleva maticí $\mathbf{A}^{-1}$.
(2) Soustava $\mathbf{AX} = \mathbf{B}$ je podle předpokladu ekvivaletní se soustavou $\mathbf{EX} = \mathbf{C}$. Řešením soustavy $\mathbf{EX} = \mathbf{C}$ je zřejmě matice $\mathbf{C}$. Protože Gaussova eliminační metoda nemění množinu řešení a podle (1) víme, že řešením obou soustav je $\mathbf{A}^{-1}\mathbf{B}$. Takže $\mathbf{C} = \mathbf{A}^{-1}\mathbf{B}$.

9.46. Poznámka. Důsledkem této věty je například metoda výpočtu inverzní matice. Inverzní matice je podle definice ?? taková matice $\mathbf{X}$, pro kterou platí $\mathbf{AX} = \mathbf{E}$. Stačí tedy v předchozí větě volit $\mathbf{B} = \mathbf{E}$.

9.47. Poznámka. Předpokládejme regulární matici $\mathbf{A} \in \mathbf{R}^{n,n}$ a soustavu lineárních rovnic $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$. Jediné řešení této soustavy můžeme počítat ze vzorce $\mathbf{A}^{-1}\boldsymbol{b}$. K výpočtu matice $\mathbf{A}^{-1}$

eliminací potřebujeme $2n^3$ operací (za jednu operaci považujeme přičtení násobku jednoho čísla k jinému). A pro maticové násobení $\mathbf{A}^{-1}\boldsymbol{b}$ potřebujeme dalších n^2 operací. Je zřejmé, že přímá úprava rozšířené matice eliminací spotřebuje nepatrně méně operací: $n^2(n+1) = n^3+n^2$ operací. Ještě méně operací potřebujeme při řešení této soustavy LU rozkladem. Postup řešení je vysvětlen v následujícím algoritmu.

9.48. Algoritmus. Nechť $\mathbf{A}$ je regulární matice, $\mathbf{AP} = \mathbf{LU}$ je její LU rozklad. Pak:

$$\mathbf{A} = \mathbf{LUP}^T, \quad \text{tedy soustavu } \mathbf{A}\boldsymbol{x} = \boldsymbol{b} \text{ lze zapsat ve tvaru } \mathbf{L}\,(\mathbf{U}\,(\mathbf{P}^T\boldsymbol{x})) = \boldsymbol{b}$$
$$\text{a řešit postupně tři soustavy: } \mathbf{L}\boldsymbol{z} = \boldsymbol{b}, \quad \mathbf{U}\boldsymbol{y} = \boldsymbol{z}, \quad \mathbf{P}^T\boldsymbol{x} = \boldsymbol{y}$$

Přitom první a třetí soustavu není nutné řešit, protože algoritmus LU rozkladu ?? poskytuje jako vedlejší produkt matici $L' = L^{-1}$ a dále platí $\mathbf{P} = (\mathbf{P}^T)^{-1}$. Takže řešíme jedinou soustavu $\mathbf{U}\,\boldsymbol{y} = \mathbf{L}'\,\boldsymbol{b}$ a podle permutační matice $\mathbf{P}$ přehodíme případně pořadí proměnných, tedy provedeme $\boldsymbol{x} = \mathbf{P}\boldsymbol{y}$.

9.49. Příklad. Řešme LU rozkladem soustavu lineárních rovnic s maticí

$$\mathbf{A} = \left(\begin{array}{ccc|c} 1 & 2 & 3 & 5 \\ 2 & 3 & 1 & 7 \\ 4 & 2 & 0 & 6 \end{array}\right)$$

LU rozklad matice této soustavy jsme provedli v příkladě ??. Takže víme, že

$$\mathbf{L}' = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 8 & -6 & 1 \end{pmatrix}, \qquad \mathbf{U} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -5 \\ 0 & 0 & 18 \end{pmatrix}, \qquad \mathbf{L}'\cdot\boldsymbol{b} = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 8 & -6 & 1 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 7 \\ 6 \end{pmatrix} = \begin{pmatrix} -$$

Soustava $\mathbf{U}\,\boldsymbol{y} = \mathbf{L}'\,\boldsymbol{b}$ má rozšířenou matici:

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 5 \\ 0 & -1 & -5 & -3 \\ 0 & 0 & 18 & 4 \end{array}\right),$$

kterou vyřešíme postupným dosazením „zespoda nahoru“: $y_3 = \frac{2}{9}$, $y_2 = \frac{17}{9}$, $y_1 = \frac{5}{9}$. Permutační matice $\mathbf{P}$ je v tomto případě jednotková, takže $x_1 = y_1$, $x_2 = y_2$, $x_3 = y_3$ a dostáváme řešení soustavy $(\frac{5}{9}, \frac{17}{9}, \frac{2}{9})$.

9.50. Poznámka. Kolik operací (přičtení násobku čísla k jinému) potřebujeme k vyřešení soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ s regulární maticí typu (n, n)? K nalezení matic $\mathbf{U}$ a $\mathbf{L}'$ potřebuje algoritmus LU rozkladu zhruba $n^3/2$ operací. K výpočtu pravé strany $\boldsymbol{z}$ potřebujeme $n^2/2$ operací a k vyřešení soustavy $\mathbf{U}\boldsymbol{y} = \boldsymbol{z}$ potřebujeme také $n^2/2$ operací. K prohození proměnných (přechod mezi vektorem $\boldsymbol{y}$ a $\boldsymbol{x}$) potřebujeme zhruba n operací, což je ve srovnání s počtem n^2 operací

pro výpočet $\boldsymbol{y}$ zanedbatelné. Shrnutí: na přípravu matice $\mathbf{A}$ (LU rozklad) je potřeba $n^3/2$ operací a na výpočet řešení pak už stačí n^2 operací.

Zdá se, že počet operací při řešení soustav pomocí LU rozkladu nebo Gaussovou eliminační metodou se příliš neliší. Ovšem jsou známy algoritmy LU rozkladu se stejnou složitostí jako násobení matic. Přitom násobení matic se dá optimalizovat tak, že potřebuje méně operací než n^3 (viz ??). Za určitých okolností při rozsáhlých soustavách může tedy být řešení soustav LU rozkladem efektivnější.

9.51. Definice. Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$. *Nulový prostor matice* $\mathbf{A}$ je lineární podprostor všech řešení homogenní soustavy lineárních rovnic $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$. Tento podprostor značíme $\operatorname{Null}\mathbf{A}$.

9.52. Poznámka. Je-li dána matice $\mathbf{A}$, pak k ní můžeme sestrojit dva lineární podprostory lineárního prostoru $\mathbf{R}^n$: nulový prostor $\operatorname{Null}\mathbf{A}$ a lineární obal řádků matice $\langle \mathrm{r}\colon \mathbf{A}\rangle$. Mezi těmito dvěma lineárními podprostory je zajímavý vztah:

9.53. Věta. Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$. Pak

(1) pro každý vektor $\boldsymbol{z} \in \operatorname{Null}\mathbf{A}$ a pro každý vektor $\boldsymbol{a} \in \langle \mathrm{r}\colon \mathbf{A}\rangle$ platí: $\boldsymbol{a} \cdot \boldsymbol{z}^T = 0$.

(2) $\langle \mathrm{r}\colon \mathbf{A}\rangle \cap \operatorname{Null}\mathbf{A} = \{\boldsymbol{o}\}$.

(3) $\dim\langle \mathrm{r}\colon \mathbf{A}\rangle + \dim \operatorname{Null}\mathbf{A} = n$.

(4) Pro každý vektor $\boldsymbol{x} \in \mathbf{R}^n$ existují jediné vektory $\boldsymbol{a} \in \langle \mathrm{r}\colon \mathbf{A}\rangle$ a $\boldsymbol{z} \in \operatorname{Null}\mathbf{A}$ tak, že $\boldsymbol{x} = \boldsymbol{a} + \boldsymbol{z}$.

Důkaz. (1) Rovnost $\boldsymbol{a}\cdot\boldsymbol{x}^T = 0$ můžeme po složkách rozepsat jako $a_1x_1+a_2x_2+\cdots+a_nx_n = 0$ a vnímat ji jako rovnici s koeficienty $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$. Protože $\boldsymbol{a} \in \langle \mathrm{r}\colon \mathbf{A}\rangle$, je $\boldsymbol{a}$ lineární kombinací řádků matice $\mathbf{A}$, tedy uvedená rovnice vznikla jako lineární kombinace rovnic ze soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$. Řešení $\boldsymbol{z} \in \operatorname{Null}\mathbf{A}$ splňuje nejen všechny rovnice ze soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{y}$, ale také všechny jejich lineární kombinace, takže platí $a_1z_1 + a_2z_2 + \cdots + a_nz_n = 0$.

(2) Je-li $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \langle \mathrm{r}\colon \mathbf{A}\rangle \cap \operatorname{Null}\mathbf{A}$, musí $x_1x_1 + x_2x_2 + \cdots + x_nx_n = x_1^2 + x_2^2 + \cdots + x_n^2 = 0$ a to je možné jen pro nulový vektor.

(3) $\dim\langle \mathrm{r}\colon \mathbf{A}\rangle$ je hodnost $\mathbf{A}$ (podle definice). Vztah byl dokázán ve větě ??.

(4) Předpokládejme, že $\operatorname{hod}\mathbf{A} = k$ a nechť $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$ je nějaká báze lineárního podprostoru $\langle \mathrm{r}\colon \mathbf{A}\rangle$ a nechť $\boldsymbol{b}_{k+1}, \boldsymbol{b}_{k+2}, \ldots, \boldsymbol{b}_n$ je báze lineárního podprostoru $\operatorname{Null}\mathbf{A}$. Pak podle věty ?? jsou vektory $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n$ lineárně nezávislé a tvoří tedy bázi lineárního prostoru $\mathbf{R}^n$. Vektor $\boldsymbol{x} \in \mathbf{R}^n$ má vzhledem k této bázi souřadnice $\alpha_1, \alpha_2, \ldots, \alpha_n$ a platí

$$\boldsymbol{x} = (\alpha_1\boldsymbol{b}_1 + \alpha_2\boldsymbol{b}_2 + \cdots + \alpha_k\boldsymbol{b}_k) + (\alpha_{k+1}\boldsymbol{b}_{k+1} + \alpha_{k+2}\boldsymbol{b}_{k+2} + \cdots + \alpha_n\boldsymbol{b}_n).$$

První závorka v tomto výrazu je rovna vektoru $\boldsymbol{a}$ a druhá vektoru $\boldsymbol{z}$. Jejich jednoznačnost plyne z jednoznačnosti souřadnic vzhledem k bázi.

9.54. Poznámka. Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$ a $\boldsymbol{a} \in \langle \mathrm{r}\colon \mathbf{A}\rangle$. Nechť $\boldsymbol{z}$ leží v nulovém prostoru matice $\mathbf{A}$. Protože $\boldsymbol{a}\cdot\boldsymbol{z}^T = \boldsymbol{z}\cdot\boldsymbol{a}^T = 0$, vidíme, že vektor $\boldsymbol{a}$ řeší homogenní rovnici s koeficienty $\boldsymbol{z} = (z_1, z_2, \ldots, z_n)$. Sestavíme matici $\mathbf{B}$, která v řádcích obsahuje bázi nulového prostoru matice $\mathbf{A}$. Pak zřejmě $\boldsymbol{a}$ řeší soustavu $\mathbf{B}\boldsymbol{x} = \boldsymbol{o}$. Takže nejen $\operatorname{Null}\mathbf{A} = \langle \mathrm{r}\colon \mathbf{B}\rangle$, ale také $\operatorname{Null}\mathbf{B} = \langle \mathrm{r}\colon \mathbf{A}\rangle$.

9.55. Shrnutí. Množina řešení soustavy lineárních rovnic je dle Frobeniovy věty /??/ prázdná, právě když hodnost rozšířené matice soustavy je větší než hodnost matice soustavy.

Množina řešení homogenní soustavy lineárních rovnic s n neznámými tvoří lineární podprostor lineárního prostoru $\mathbf{R}^n$ /??/. Dimenze tohoto podprostoru je rovna $n - \hod \mathbf{A}$, kde $\mathbf{A}$ je matice soustavy a n je počet neznámých /??/.

Množina řešení nehomogenní soustavy lineárních rovnic se dá zapsat jako součet patrikulárního řešení a množiny řešení přidružené homogenní soustavy /??, ??/.

V této kapitole jsme si ukázali algoritmus na hledání báze množiny řešení přidružené homogenní soustavy i na hledání partikulárního řešení /??, ??/.

Množina řešení soustavy lineárních rovnic tvoří z geometrického pohledu zobecněnou rovinu, která je průnikem zobecněných rovin, které jsou řešeními jednotlivých rovnic /??, ??/. Je to také zobecněná rovina, která vzniká posunutím zobecněné roviny popisující množinu řešení přidružené homogenní soustavy z počátku o vektor partikulárního řešení

Množinu řešení soustav lineárních rovnic nelze popsat jednoznačně /??, ??/. Posali jsme si algritmus, podle kterého poznáme, že dva na první pohled různé zápisy popisují stejnou množinu řešení.

Soustavy se čtvercovou maticí mají svou matici singulární (pak po eliminaci už nemají čtvercovou matici), nebo regulární. Ta má jediné řešení ve tvaru $\mathbf{A}^{-1}\boldsymbol{b}$. Jednotlivé složky takového řešení se dají spočítat jako podíl determinantů /Cramerovo pravidlo ??/.

Vyřešit maticovou rovnici $\mathbf{AX} = \mathbf{B}$ znamená totéž, jako vyřešit soustavu soustav se stejnou maticí soustavy a s různými pravými stranami /??/. Eliminace $(\mathbf{A}\,|\,\mathbf{B}) \sim (\mathbf{E}\,|\,\mathbf{C})$

počítá součin $\mathbf{C} = \mathbf{A}^{-1}\,\mathbf{B}$, což je jediné řešení soustavy $\mathbf{AX} = \mathbf{B}$ v případě, že matice $\mathbf{A}$ je regulární /??/.

V závěru kapitoly jsme ukázali řešení soustav lineárních rovnic LU rozkladem.

10. Matice lineárního zobrazení

10.1. Věta. Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$ je matice. Pak zobrazení $\mathcal{A}\colon \mathbf{R}^n \to \mathbf{R}^m$ definované předpisem $\mathcal{A}(\boldsymbol{x}) = \mathbf{A} \cdot \boldsymbol{x}$ je lineární.

Důkaz. Podle definice ?? stačí ověřit, že

$$\mathbf{A} \cdot (\boldsymbol{x} + \boldsymbol{y}) = \mathbf{A} \cdot \boldsymbol{x} + \mathbf{A} \cdot \boldsymbol{y}, \qquad \mathbf{A} \cdot (\alpha \boldsymbol{x}) = \alpha(\mathbf{A} \cdot \boldsymbol{x}),$$

což platí díky větě ??.

10.2. Poznámka. Zobrazení v předchozí větě zobrazuje sloupcové vektory na sloupcové vektory, tedy přesněji bychom měli psát $\mathcal{A}\colon \mathbf{R}^{n,1} \to \mathbf{R}^{m,1}$. Ovšem vzhledem k izomorfismu mezi $\mathbf{R}^{n,1}$ a $\mathbf{R}^n$ (viz poznámku ??) nebudeme dále tuto skutečnost zbytečně zdůrazňovat.

10.3. Příklad. Najdeme jádro, defekt a hodnost zobrazení $\mathcal{A}\colon \mathbf{R}^4 \to \mathbf{R}^3$, které je dáno předpisem $\mathcal{A}(x_1, x_2, x_3, x_4) = (x_1 + 3x_2 + 2x_3 + 2x_4, 3x_1 + x_2 + 2x_4, 5x_1 + 7x_2 + 4x_3 + 6x_4)$.

Ze vzorce pro hodnotu zobrazení okamžitě plyne, že

$$\mathcal{A}(x_1, x_2, x_3, x_4)^T = \begin{pmatrix} x_1 + 3x_2 + 2x_3 + 2x_4 \\ 3x_1 + x_2 + 2x_4 \\ 5x_1 + 7x_2 + 4x_3 + 6x_4 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 & 2 \\ 3 & 1 & 0 & 2 \\ 5 & 7 & 4 & 6 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \mathbf{A} \cdot \boldsymbol{x}$$

takže $\mathcal{A}(\boldsymbol{x}) = \mathbf{A} \cdot \boldsymbol{x}$, kde $\mathbf{A} \in \mathbf{R}^{3,4}$.

Hodnost zobrazení $\mathcal{A}$ je podle definice ?? rovna dimenzi lineárního podprostoru všech hodnot zobrazení a tento podprostor je roven lineárnímu obalu všech obrazů bázových vektorů. Ve vstupním lineárním prostoru použijeme strandardní bázi. Platí

$$\mathcal{A}(1,0,0,0) = (1,3,5), \quad \mathcal{A}(0,1,0,0) = (3,1,7), \quad \mathcal{A}(0,0,1,0) = (2,0,4), \quad \mathcal{A}(0,0,0,1) = (2,2,6$$

Všimneme si, že díky vlastnostem maticového násobení jsou obrazy bázových vektorů rovny jednotlivým sloupcům matice $\mathbf{A}$. Hodnost zobrazení $\mathcal{A}$ je tedy rovna lineárnímu obalu sloupců matice $\mathbf{A}$, ale protože podle věty ?? je $\operatorname{hod} \mathbf{A} = \operatorname{hod} \mathbf{A}^T$, stačí počítat dimenzi lineárního obalu řádků matice $\mathbf{A}$, neboli hodnost matice $\mathbf{A}$.

$$\mathbf{A} = \begin{pmatrix} 1 & 3 & 2 & 2 \\ 3 & 1 & 0 & 2 \\ 5 & 7 & 4 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 2 & 2 \\ 0 & 8 & 6 & 4 \end{pmatrix}, \qquad \operatorname{hod} \mathbf{A} = 2$$

Je tedy $\operatorname{hod} \mathcal{A} = \operatorname{hod} \mathbf{A} = 2$.

Jádro zobrazení $\mathcal{A}$ je podle definice ?? množina všech $\boldsymbol{x} \in \mathbf{R}^4$ takových, že $\mathbf{A} \cdot \boldsymbol{x} = \boldsymbol{o}$. Je to tedy lineární podprostor všech řešení homogenní soustavy rovnic s maticí $\mathbf{A}$. Řešit soustavy

lineárních rovnic umíme:

$$\begin{pmatrix} 1 & 3 & 2 & 2 \\ 3 & 1 & 0 & 2 \\ 5 & 7 & 4 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 2 & 2 \\ 0 & 1 & 3/4 & 1/2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -1/4 & 1/2 \\ 0 & 1 & 3/4 & 1/2 \end{pmatrix} = (\mathbf{E} \mid \mathbf{C}),$$

$$(-\mathbf{C}^T \mid \mathbf{E}) = \begin{pmatrix} 1/4 & -3/4 & 1 & 0 \\ -1/2 & -1/2 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & -3 & 4 & 0 \\ 1 & 1 & 0 & -2 \end{pmatrix}$$

Při výpočtu jsme použili větu ??. $\operatorname{Ker} \mathcal{A} = \langle (1,-3,4,0), (1,1,0,-2) \rangle$, $\operatorname{def} \mathcal{A} = \dim \operatorname{Ker} \mathcal{A} = 2$.

Tento příklad ilustruje lineární zobrazení, které není prosté (protože $\operatorname{def} \mathcal{A} > 0$) a také není „na“ $\mathbf{R}^3$ (protože $\dim \mathbf{R}^3 = 3$, ale $\operatorname{hod} \mathcal{A} = 2$).

10.4. Věta. Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$. Hodnost lineárního zobrazení $\mathcal{A} \colon \mathbf{R}^n \to \mathbf{R}^m$, které je dáno předpisem $\mathcal{A}(\boldsymbol{x}) = \mathbf{A} \cdot \boldsymbol{x}$, je rovna hodnosti matice $\mathbf{A}$, tedy:

$$\operatorname{hod} \mathcal{A} = \operatorname{hod} \mathbf{A}$$

Důkaz. Důkaz povedeme stejně, jako když jsme počítali hodnost zobrazení v předchozím příkladu. Nechť $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n\}$ je standardní báze lineárního prostoru $\mathbf{R}^n$. Díky vlastnostem maticového násobení je $\mathbf{A} \cdot \boldsymbol{e}_i$ rovno i-tému sloupci matice $\mathbf{A}$. Podle definic ?? a ?? platí:

$$\operatorname{hod} \mathcal{A} = \dim \mathcal{A}(\mathbf{R}^n) = \dim \mathcal{A}(\langle \boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n \rangle) = \dim \langle \mathcal{A}(\boldsymbol{e}_1), \mathcal{A}(\boldsymbol{e}_2), \ldots, \mathcal{A}(\boldsymbol{e}_n) \rangle = \operatorname{hod} \mathbf{A}^T = \text{hod}$$

10.5. Poznámka. Je-li dána matice $\mathbf{A} \in \mathbf{R}^{m,n}$, pak jádrem lineárního zobrazení $\mathbf{A} \cdot \boldsymbol{x}$ je lineární podprostor všech řešení homogenní soustavy $\mathbf{A} \cdot \boldsymbol{x} = \boldsymbol{o}$, tedy její nulový prostor $\operatorname{Null} \mathbf{A}$.

10.6. Poznámka. Věta ?? „$\operatorname{def} \mathcal{A} + \operatorname{hod} \mathcal{A} = \dim L_1$“ přechází v případě zobrazení typu $\mathbf{A} \cdot \boldsymbol{x}$ na větu ?? „$\dim \operatorname{Null} \mathbf{A} + \operatorname{hod} \mathbf{A} =$ počet neznámých soustavy lineárních rovnic s maticí $\mathbf{A}$“. Defekt je totiž dimenze kernelu, což je dimenze nulového prostoru matice $\mathbf{A}$. Hodnost zobrazení je dle věty ?? rovna hodnosti matice. Konečně $\dim L_1$ je rovna počtu sloupců v matici $\mathbf{A}$, tedy počtu neznámých soustavy.

10.7. Poznámka. V následujícím textu na chvíli opustíme zobrazení typu $\mathbf{A} \cdot \boldsymbol{x}$, abychom se k němu později znovu vrátili obohaceni o další poznatky o obecných lineárních zobrazeních. Pak už budeme moci dokázat, že každé lineární zobrazení lineárních prostorů konečné dimenze je (až na izomorfismus) zobrazení typu $\mathbf{A} \cdot \boldsymbol{x}$, kde $\mathbf{A}$ je nějaká matice.

10.8. Poznámka. Nechť L_1 a L_2 jsou lineární prostory. Symbolem T označme množinu všech lineárních zobrazení z L_1 do L_2. V následující definici zavedeme součet dvou zobrazení, které jsou prvky množiny T, a α-násobek takového zobrazení. Ve větě ?? pak dokážeme, že množina T s těmito operacemi tvoří lineární prostor.

10.9. Definice. Nechť $\mathcal{A}\colon L_1 \to L_2$, $\mathcal{B}\colon L_1 \to L_2$ jsou lineární zobrazení a $\alpha \in \mathbf{R}$. Pak definujeme součet lineárních zobrazení $\mathcal{A}+\mathcal{B}\colon L_1 \to L_2$ předpisem $(\mathcal{A}+\mathcal{B})(\boldsymbol{x}) = \mathcal{A}(\boldsymbol{x})+\mathcal{B}(\boldsymbol{x})$ pro všechna $\boldsymbol{x} \in L_1$. Dále definujeme α-násobek zobrazení $\mathcal{A}$ jako zobrazení $\alpha\mathcal{A}\colon L_1 \to L_2$, které splňuje $(\alpha\mathcal{A})(\boldsymbol{x}) = \alpha\mathcal{A}(\boldsymbol{x})$ pro všechna $\boldsymbol{x} \in L_1$.

10.10. Věta. Nechť L_1 a L_2 jsou lineární prostory a označme $T = \{\mathcal{A}\colon L_1 \to L_2\}$. Pak T s operacemi podle definice ?? je lineární prostor.

Důkaz. Nejprve je potřeba dokázat, že součet lineárních zobrazení je lineární zobrazení a α násobek lineárního zobrazení je také lineární zobrazení. Tedy pro ně musí platit vlastnosti (1) a (2) z definice ??. Nechť $\mathcal{A} \in T, \mathcal{B} \in T, \alpha \in \mathbf{R}$. Pro $\boldsymbol{x} \in L_1, \boldsymbol{y} \in L_1$ a $\gamma \in \mathbf{R}$ platí:

(1) $(\mathcal{A}+\mathcal{B})(\boldsymbol{x}+\boldsymbol{y}) = \mathcal{A}(\boldsymbol{x}+\boldsymbol{y}) + \mathcal{B}(\boldsymbol{x}+\boldsymbol{y}) = \big(\mathcal{A}(\boldsymbol{x}) + \mathcal{A}(\boldsymbol{y})\big) + \big(\mathcal{B}(\boldsymbol{x}) + \mathcal{B}(\boldsymbol{y})\big) =$
$= \big(\mathcal{A}(\boldsymbol{x}) + \mathcal{B}(\boldsymbol{x})\big) + \big(\mathcal{A}(\boldsymbol{y}) + \mathcal{B}(\boldsymbol{y})\big) = (\mathcal{A}+\mathcal{B})(\boldsymbol{x}) + (\mathcal{A}+\mathcal{B})(\boldsymbol{y}),$

(2) $(\mathcal{A}+\mathcal{B})(\gamma\boldsymbol{x}) = \mathcal{A}(\gamma\boldsymbol{x}) + \mathcal{B}(\gamma\boldsymbol{x}) = \gamma\mathcal{A}(\boldsymbol{x}) + \gamma\mathcal{B}(\boldsymbol{x}) = \gamma\big(\mathcal{A}(\boldsymbol{x}) + \mathcal{B}(\boldsymbol{x})\big) = \gamma(\mathcal{A}+\mathcal{B})(\boldsymbol{x}),$
tj. $\mathcal{A}+\mathcal{B}$ je lineární,

(1) $(\alpha\mathcal{A})(\boldsymbol{x}+\boldsymbol{y}) = \alpha\mathcal{A}(\boldsymbol{x}+\boldsymbol{y}) = \alpha\big(\mathcal{A}(\boldsymbol{x}) + \mathcal{A}(\boldsymbol{y})\big) = \alpha\mathcal{A}(\boldsymbol{x}) + \alpha\mathcal{A}(\boldsymbol{y}) = (\alpha\mathcal{A})(\boldsymbol{x}) + (\alpha\mathcal{A})(\boldsymbol{y}),$

(2) $(\alpha\mathcal{A})(\gamma\boldsymbol{x}) = \alpha\mathcal{A}(\gamma\boldsymbol{x}) = \alpha\big(\gamma\mathcal{A}(\boldsymbol{x})\big) = (\alpha\gamma)\mathcal{A}(\boldsymbol{x}) = \gamma\big(\alpha\mathcal{A}(\boldsymbol{x})\big) = \gamma(\alpha\mathcal{A})(\boldsymbol{x}),$
tj. $\alpha\mathcal{A}$ je lineární.

Dále je třeba dokázat, že pro operace + a · z definice ?? platí axiomy linearity, tedy vlastnosti (1) až (7) z definice ??. Argumentace je zcela stejná, jako v příkadu ??, takže ji zde nebudeme opakovat. Rozdíl je jen v tom, že se při argumentaci neopíráme o vlastnosti sčítání a násobení reálných čísel, ale opíráme se o axiomy linearity, které platí v lineárním prostoru L_2.

10.11. Poznámka. Následující věta ukazuje, že pokud známe hodnoty zobrazení $\mathcal{A}\colon L_1 \to L_2$ jen na bázi lineárního prostoru L_1 a toto zobrazení má být lineární, pak takové zobrazení existuje a je hodnotami na bázi jednoznačně určeno.

10.12. Věta.* Nechť $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ je báze lineárního prostoru L_1 a nechť jsou dány libovolné vektory $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_n$ z lineárního prostoru L_2. Pak existuje právě jedno lineární zobrazení $\mathcal{A}\colon L_1 \to L_2$, pro které platí

$$\mathcal{A}(\boldsymbol{b}_i) = \boldsymbol{y}_i, \quad \forall i \in \{1, 2, \ldots, n\}. \tag{10.1}$$

Důkaz. (1) Existence. Nechť $\boldsymbol{x} \in L_1$. Protože $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ je báze L_1, existují souřadnice $\alpha_i \in \mathbf{R}$ vektoru $\boldsymbol{x}$ takové, že $\boldsymbol{x} = \alpha_1 \boldsymbol{b}_1 + \alpha_2 \boldsymbol{b}_2 + \cdots + \alpha_n \boldsymbol{b}_n$. Hodnotu zobrazení $\mathcal{A}$ v bodě $\boldsymbol{x}$ nyní definujeme takto:

$$\mathcal{A}(\boldsymbol{x}) = \alpha_1 \boldsymbol{y}_1 + \alpha_2 \boldsymbol{y}_2 + \cdots + \alpha_n \boldsymbol{y}_n. \tag{10.2}$$

Zobrazení, které vektorům přiřazuje jejich souřadnice, je lineární (viz větu ??). Z toho plyne, že zobrazení $\mathcal{A}$ definované vzorcem (10.2) je lineární. Pečlivější čtenář si to rozepíše podrobněji.

Protože souřadnice vektoru $\boldsymbol{b}_i$ vzhledem k bázi (B) jsou všechny nulové s výjimkou i-té souřadnice, která je rovna jedné, platí

$$\mathcal{A}(\boldsymbol{b}_i) = \sum_{\substack{j=0 \\ j\neq i}}^{n} 0 \cdot \boldsymbol{y}_j + 1 \cdot \boldsymbol{y}_i = \boldsymbol{y}_i,$$

takže zobrazení definované vzorcem (10.2) splňuje požadovanou vlastnost (10.1).

(2) Jednoznačnost. Nechť ještě $\mathcal{B}\colon L_1 \to L_2$ je lineární a splňuje vlastnost (10.1). Pak je lineární i zobrazení $(\mathcal{A}-\mathcal{B})\colon L_1 \to L_2$, protože množina lineárních zobrazení tvoří podle věty ?? lineární prostor. Platí $(\mathcal{A}-\mathcal{B})(\boldsymbol{b}_i) = \boldsymbol{o}\ \forall i \in \{1,2,\ldots,n\}$, protože $\mathcal{A}$ i $\mathcal{B}$ splňují vlastnost (10.1). Z linearity zobrazení $\mathcal{A}-\mathcal{B}$ plyne, že

$$\begin{aligned}(\mathcal{A}-\mathcal{B})(\boldsymbol{x}) &= (\mathcal{A}-\mathcal{B})(\alpha_1\,\boldsymbol{b}_1 + \alpha_2\,\boldsymbol{b}_2 + \cdots + \alpha_n\,\boldsymbol{b}_n) = \\ &= \alpha_1\,(\mathcal{A}-\mathcal{B})(\boldsymbol{b}_1) + \alpha_2\,(\mathcal{A}-\mathcal{B})(\boldsymbol{b}_2) + \cdots + \alpha_n\,(\mathcal{A}-\mathcal{B})(\boldsymbol{b}_n) = \\ &= \alpha_1\,\boldsymbol{o} + \alpha_2\,\boldsymbol{o} + \cdots + \alpha_n\,\boldsymbol{o} = \boldsymbol{o}.\end{aligned}$$

Vidíme, že zobrazení $\mathcal{A}-\mathcal{B}$ je nulové na celém definičním oboru, takže $\mathcal{A}=\mathcal{B}$.

10.13. Poznámka. V důkazu věty ?? jsme uvedli důležitý vzorec (10.2), který ukazuje, jak najít hodnotu lineárního zobrazení pro libovolný vektor $\boldsymbol{x} \in L_1$, známe-li hodnoty tohoto zobrazení jen na nějaké bázi lineárního prostoru L_1.

10.14. Příklad. Předpokládejme, že $\mathcal{A}\colon \mathbf{R}^3 \to \mathbf{R}^4$ je lineární zobrazení. Najdeme vzorec pro výpočet hodnoty zobrazení $\mathcal{A}(x_1, x_2, x_3)$, je-li známo:

$$\mathcal{A}(1,1,2) = (1,0,1,0), \quad \mathcal{A}(1,2,2) = (2,0,2,0), \quad \mathcal{A}(2,1,5) = (1,2,2,1).$$

Protože jsou vektory $(1,1,2), (1,2,2), (2,1,5)$ lineárně nezávislé a jsou tři, tvoří podle poznámky ?? bázi lineárního prostoru $\mathbf{R}^3$. Známe hodnoty hledaného zobrazení na bázi $\mathbf{R}^3$, takže podle věty ?? můžeme jednoznačně určit hodnoty $\mathcal{A}$ i v ostatních bodech definičního oboru. Budeme postupovat stejně, jako v důkazu věty ??.

Nechť (x_1, x_2, x_3) je libovolný vektor z $\mathbf{R}^3$. Najdeme souřadnice tohoto vektoru vzhledem k uspořádané bázi $\big((1,1,2), (1,2,2), (2,1,5)\big)$:

$$(x_1, x_2, x_3) = \alpha\,(1,1,2) + \beta\,(1,2,2) + \gamma\,(2,1,5).$$

To vede na soustavu tří rovnic o třech neznámých α, β, γ. Eliminujme její rozšířenou matici:

$$\left(\begin{array}{ccc|c} 1 & 1 & 2 & x_1 \\ 1 & 2 & 1 & x_2 \\ 2 & 2 & 5 & x_3 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & 2 & x_1 \\ 0 & 1 & -1 & x_2 - x_1 \\ 0 & 0 & 1 & x_3 - 2x_1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 0 & 8x_1 - x_2 - 3x_3 \\ 0 & 1 & 0 & -3x_1 + x_2 + x_3 \\ 0 & 0 & 1 & x_3 - 2x_1 \end{array}\right).$$

Platí tedy

$$\begin{aligned}
(x_1,x_2,x_3) &= (8x_1-x_2-3x_3)\cdot(1,1,2)+(-3x_1+x_2+x_3)\cdot(1,2,2)+(x_3-2x_1)\cdot(2,1,5),\\
\mathcal{A}(x_1,x_2,x_3) &= \mathcal{A}\big((8x_1-x_2-3x_3)\cdot(1,1,2)+(-3x_1+x_2+x_3)\cdot(1,2,2)+(x_3-2x_1)\cdot(2,1,5\\
&= (8x_1-x_2-3x_3)\cdot\mathcal{A}(1,1,2)+(-3x_1+x_2+x_3)\cdot\mathcal{A}(1,2,2)+(x_3-2x_1)\cdot\mathcal{A}(2,\\
&= (8x_1-x_2-3x_3)\cdot(1,0,1,0)+(-3x_1+x_2+x_3)\cdot(2,0,2,0)+(x_3-2x_1)\cdot(1,2,\\
&= (x_2,\ -4x_1+2x_3,\ -2x_1+x_2+x_3,\ -2x_1+x_3).
\end{aligned}$$

10.15. Věta. Pro každé lineární zobrazení $\mathcal{A}\colon \mathbf{R}^n \to \mathbf{R}^m$ existuje právě jedna matice $\mathbf{A} \in \mathbf{R}^{m,n}$ taková, že $\mathcal{A}(\boldsymbol{x}) = \mathbf{A}\cdot\boldsymbol{x}$.

Důkaz. Nechť je dáno zobrazení $\mathcal{A}\colon \mathbf{R}^n \to \mathbf{R}^m$. Označme $(S_n) = (\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n)$ standardní bázi v $\mathbf{R}^n$. Hodnoty $\mathcal{A}(\boldsymbol{e}_i)$ pro $i = \{1, 2, \ldots, n\}$ zapišme jako sloupcové vektory vedle sebe do matice, kterou označíme $\mathbf{A}$. Tedy $\mathbf{A} = \big(\mathcal{A}(\boldsymbol{e}_1)\ \mathcal{A}(\boldsymbol{e}_2)\ \ldots\ \mathcal{A}(\boldsymbol{e}_n)\big)$. Je zřejmé, že zobrazení, které vektoru $\boldsymbol{x}$ přiřadí vektor $\mathbf{A}\cdot\boldsymbol{x}$, má pro $\boldsymbol{x} \in \{\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n\}$ stejné hodnoty, jako dané zobrazení $\mathcal{A}$. Podle věty ?? existuje jediné lineární zobrazení s takovou vlastností.

Proč je matice $\mathbf{A}$ zobrazením $\mathcal{A}$ jednoznačně určena? Jiná matice odpovídá zobrazení, které má jiné hodnoty pro $\boldsymbol{x} \in \{\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n\}$, takže to je jiné zobrazení.

10.16. Definice. Nechť $\mathcal{A}\colon \mathbf{R}^n \to \mathbf{R}^m$ je lineární zobrazení. Matici $\mathbf{A}$, pro kterou je $\mathbf{A}\cdot\boldsymbol{x} = \mathcal{A}(\boldsymbol{x})\ \forall \boldsymbol{x} \in \mathbf{R}^n$, nazýváme *maticí lineárního zobrazení* $\mathcal{A}$.

10.17. Poznámka. Důkaz věty ?? dává návod, jak matici zobrazení $\mathcal{A}$ sestavit. Do sloupců matice je třeba zapsat obrazy vektorů standardní báze.

10.18. Příklad. V příkladu ?? jsme měli zobrazení $\mathcal{A}\colon \mathbf{R}^3 \to \mathbf{R}^4$ dáno hodnotami na bázi a vypočítali jsme, že $\mathcal{A}(x_1, x_2, x_3) = (x_2,\ -4x_1 + 2x_3,\ -2x_1 + x_2 + x_3,\ -2x_1 + x_3)$. Nyní najdeme jeho matici, hodnost, jádro a defekt.

Matici můžeme hledat dvěma způsoby. Obrazy bázových vektorů standardní báze musejí být zapsány postupně do sloupců matice $\mathbf{A}$. Nebo jinak: koeficienty lineárních kombinací jednotlivých složek obrazu vektoru (x_1, x_2, x_3) musejí být zapsány do řádků matice $\mathbf{A}$. Vyzkoušejte si oba přístupy. Takže:

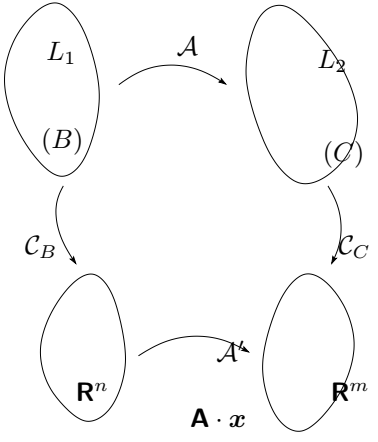
$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 \\ -4 & 0 & 2 \\ -2 & 1 & 1 \\ -2 & 0 & 1 \end{pmatrix}$$

Hodnost zobrazení je rovna hodnosti jeho matice (věta ??), jádro zobrazení je rovno nulovému prostoru jeho matice a defekt je roven $\dim \mathbf{R}^n - \operatorname{hod} \mathcal{A}$. Níže jsou uvedeny s tím související

výpočty.

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 \\ -4 & 0 & 2 \\ -2 & 1 & 1 \\ -2 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \begin{array}{l} \operatorname{hod} \mathcal{A} = \operatorname{hod} \mathbf{A} = 2 \\ \operatorname{def} \mathcal{A} = 3 - \operatorname{hod} \mathcal{A} = 1,\ \operatorname{Ker} \mathcal{A} = \operatorname{Null} \mathbf{A} = \langle (1,0,2) \rangle. \end{array}$$

10.19. Poznámka. V definici ?? jsme přiřadili matici každému lineárnímu zobrazení z $\mathbf{R}^n$ do $\mathbf{R}^m$. Omezili jsme se tedy na zobrazení, která zobrazují uspořádané n-tice na uspořádané m-tice. V následující definici zavedeme matici lineárního zobrazení libovolných lineárních prostorů konečné dimenze.



10.20. Definice.* Nechť $\mathcal{A} \colon L_1 \to L_2$ je lineární zobrazení a předpokládejme, že $\dim L_1 = n$ a $\dim L_2 = m$. Věta ?? nám zaručuje, že L_1 je izomorfní s $\mathbf{R}^n$ a L_2 je izomorfní s $\mathbf{R}^m$. V lineárním prostoru L_1 zvolme nějakou uspořádanou bázi (B) a v lineárním prostoru L_2 zvolme uspořádanou bázi (C). Označme $\mathcal{C}_B \colon L_1 \to \mathbf{R}^n$ izomorfismus, který přiřazuje vektoru $\boldsymbol{u} \in L_1$ jeho souřadnice vzhledem k uspořádané bázi

(B). Nechť dále $\mathcal{C}_C : L_2 \to \mathbf{R}^m$ je izomorfismus, který přiřazuje vektoru $\boldsymbol{v} \in L_2$ jeho souřadnice vzhledem k uspořádané bázi (C). Složené zobrazení $\mathcal{A}' = \mathcal{C}_C \circ \mathcal{A} \circ \mathcal{C}_B^{-1}$ je zobrazením z $\mathbf{R}^n$ do $\mathbf{R}^m$ a má tedy podle věty ?? svou matici $\mathbf{A} \in \mathbf{R}^{m,n}$. Tuto matici nazýváme *maticí zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C)* a značíme ji $\mathbf{A} = \mathcal{M}_{B,C}(\mathcal{A})$.

10.21. Věta.* Nechť $\mathcal{A}\colon L_1 \to L_2$ je lineární zobrazení, $\dim L_1 = n$ a $\dim L_2 = m$. Nechť (B) je uspořádaná báze v L_1 a (C) je uspořádaná báze v L_2. Nechť $\mathbf{A} = \mathcal{M}_{B,C}(\mathcal{A})$ je matice zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C). Nechť $\boldsymbol{u} \in L_1$, $\boldsymbol{v} \in L_2$, $\mathcal{A}(\boldsymbol{u}) = \boldsymbol{v}$. Nechť $\boldsymbol{x} = \mathcal{C}_B(\boldsymbol{u})^T$ jsou souřadnice vektoru $\boldsymbol{u}$ vzhledem k bázi (B) a $\boldsymbol{y} = \mathcal{C}_C(\boldsymbol{v})^T$ jsou souřadnice vektoru $\boldsymbol{v}$ vzhledem k bázi (C). Pak $\mathbf{A} \cdot \boldsymbol{x} = \boldsymbol{y}$. Lapidárně řečeno, pro každé $\boldsymbol{u} \in L_1$ platí:

$$\mathbf{A} \cdot \begin{pmatrix} \text{souřadnice} \\ \text{vektoru} \\ \boldsymbol{u} \\ \text{vzhledem} \\ \text{k } (B) \end{pmatrix} = \begin{pmatrix} \text{souřadnice} \\ \text{vektoru} \\ \mathcal{A}(\boldsymbol{u}) \\ \text{vzhledem} \\ \text{k } (C) \end{pmatrix} \tag{10.3}$$

Obráceně: každá matice $\mathbf{A} \in \mathbf{R}^{m,n}$, která splňuje (10.3) pro všechny vektory $\boldsymbol{u} \in L_1$, je maticí zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C).

Důkaz. Věta je jen v jiné formě zapsaná definice ?? matice lineárního zbrazení vzhledem k bázím (B) a (C). Zobrazení $\mathcal{A}'$ z této definice zobrazuje souřadnice vektoru $\boldsymbol{u}$ vzhledem

k bázi (B) na souřadnice vektoru $\mathcal{A}(\boldsymbol{u})$ vzhledem k bázi (C), tedy zobrazí $\boldsymbol{x}$ na $\boldsymbol{y}$. Matice $\mathbf{A}$ zobrazení $\mathcal{A}'$ podle definice ?? splňuje $\mathbf{A} \cdot \boldsymbol{x} = \boldsymbol{y}$.

Obráceně: stačí ukázat, že nemohou existovat dvě různé matice splňující (10.3) pro všechna $\boldsymbol{u} \in L_1$. Označme $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ a dosadíme do rovnosti (10.3) postupně $\boldsymbol{u} = \boldsymbol{b}_i$. Souřadnice vektoru $\boldsymbol{b}_i$ vzhledem k bázi (B) je vektor $\boldsymbol{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)^T$, kde jednička je v i-té složce. Maticové násobení $\mathbf{A} \cdot \boldsymbol{e}_i$ je rovno i-tému sloupci matice $\mathbf{A}$. Takže matice $\mathbf{A}$ musí v i-tém sloupci obsahovat souřadnice vektoru $\mathcal{A}(\boldsymbol{b}_i)$ vzhledem k bázi (C). Taková matice je jenom jediná a je zřejmě maticí zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C).

10.22. Věta.* Nechť $\mathcal{A}\colon L_1 \to L_2$ je lineární zobrazení. Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je uspořádaná báze v L_1 a $(C) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m)$ je uspořádaná báze v L_2. Matice $\mathbf{A}$ je maticí zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C) právě tehdy, když obsahuje v i-tém sloupci souřadnice vektoru $\mathcal{A}(\boldsymbol{b}_i)$ vzhledem k bázi (C) pro všechna $i \in \{1, 2, \ldots, n\}$.

Důkaz. Viz druhou část důkazu předchozí věty.

10.23. Věta.* Nechť $\mathcal{A}\colon L_1 \to L_2$ je lineární zobrazení. Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je uspořádaná báze v L_1 a $(C) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m)$ je uspořádaná báze v L_2. Matice $\mathbf{A}$ je maticí zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C) právě tehdy, když splňuje maticovou rovnost

$$\big(\mathcal{A}(\boldsymbol{b}_1) \;\; \mathcal{A}(\boldsymbol{b}_2) \;\; \ldots \;\; \mathcal{A}(\boldsymbol{b}_n)\big) = (\boldsymbol{c}_1 \;\; \boldsymbol{c}_2 \;\; \ldots \;\; \boldsymbol{c}_m) \cdot \mathbf{A}. \tag{10.4}$$

Uvedenou rovnost čteme takto: jednořádková matice s obrazy bázových vektorů $\mathcal{A}(\boldsymbol{b}_i)$ je rovna součinu jednořádkové matice s bázovými vektory $\boldsymbol{c}_i$ a matice $\mathbf{A} \in \mathbf{R}^{m,n}$.

Důkaz. Matice $\mathbf{A}$ splňuje rovnost (10.4) právě tehdy, když i-tý sloupec matice $\mathbf{A}$ obsahuje souřadnice vektoru $\mathcal{A}(\boldsymbol{b}_i)$ vzhledem k bázi (C). Stačí si rozepsat maticové násobení na pravé straně rovnosti (10.4) po sloupcích matice $\mathbf{A}$. Dále použijeme větu ??.

10.24. Poznámka. Matici zobrazení jsme definovali jednak v definici ?? a také v definici ??. Je zřejmé, že matice zobrazení bez uvedení bází (podle definice ??) je z pohledu definice ?? maticí zobrazení vzhledem ke standardním bázím (S_n) v $\mathbf{R}^n$ a (S_m) v $\mathbf{R}^m$. Je to z toho důvodu, že složky vektoru z $\mathbf{R}^n$ jsou podle věty ?? rovny souřadnicím vektoru vzhledem ke standardní bázi.

Domluvíme se na tom, že pokud budeme pracovat s lineárními zobrazeními $\mathbf{R}^n \to \mathbf{R}^m$ a pouze se standardními bázemi v $\mathbf{R}^n$ a $\mathbf{R}^m$, pak nemusíme v případě matice zobrazení explicitně mluvit o bázích (jako v definici ??). V ostatních případech budeme báze v souvislosti s maticí zobrazení vždy uvádět.

10.25. Příklad. Nechť L_1 je lineární prostor všech polynomů nejvýše třetího stupně a L_2 je lineární prostor všech polynomů nejvýše druhého stupně. Uvažujme zobrazení $\mathcal{A}\colon L_1 \to L_2$, které derivuje polynomy, tedy $\mathcal{A}(p) = p'$. Toto zobrazení je zřejmě lineární. V lineárním

prostoru L_1 zvolme uspořádanou bázi $(B) = (1, x, x^2, x^3)$ a v lineárním prostoru L_2 zvolme uspořádanou bázi $(C) = (1, x, x^2)$. Najdeme matici zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C).

Obrazy bázových vektorů jsou: $\mathcal{A}(1) = 0$, $\mathcal{A}(x) = 1$, $\mathcal{A}(x^2) = 2x$, $\mathcal{A}(x^3) = 3x^2$. Souřadnice těchto obrazů vzhledem k bázi (C) jsou: $\mathcal{C}_C(0) = (0,0,0)$, $\mathcal{C}_C(1) = (1,0,0)$, $\mathcal{C}_C(2x) = (0,2,0)$, $\mathcal{C}_C(3x^2) = (0,0,3)$. Abychom získali matici zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C), je potřeba podle věty ?? uvedené souřadnice zapsat do sloupců:

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

Zkusme nyní derivovat polynomy pomocí maticového násobení. Polynom $ax^3 + bx^2 + cx + d$ má v uspořádané bázi (B) souřadnice (d, c, b, a). Souřadnice jeho obrazu (tj. v tomto příkladě jeho derivace) vzhledem k uspořádané bázi (C) najdeme podle věty ?? maticovým násobením:

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} d \\ c \\ b \\ a \end{pmatrix} = \begin{pmatrix} c \\ 2b \\ 3a \end{pmatrix}$$

tedy zderivovaný polynom je $3ax^2 + 2bx + c$.

10.26. Příklad. Najdeme matici zobrazení $\mathcal{A}\colon \mathbf{R}^3 \to \mathbf{R}^4$ z příkladu ?? vzhledem k uspořádaným bázím (B) a (S_4), kde $(B) = \big((1,1,2),(1,2,2),(2,1,5)\big)$ a (S_4) je standardní báze v $\mathbf{R}^4$.

Protože souřadnice vektorů z $\mathbf{R}^4$ vzhledem ke standardní bázi S_4 jsou přímo rovny složkám těchto vektorů (viz větu ??), stačí napsat složky obrazů vektorů z (B) do sloupců matice. Tyto obrazy jsou přímo v zadání příkladu:

$$\mathcal{M}_{B,S_4}(\mathcal{A}) = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 2 \\ 1 & 2 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Povšimneme si, že k sestavení této matice jsme nepotřebovali znát vzorec pro $\mathcal{A}(x_1,x_2,x_3)$, stačilo sepsat do sloupců matice údaje, které byly obsahem zadání příkladu. Na druhé straně k sestavení matice $\mathcal{M}_{S_3,S_4}$ (viz příklad ??) jsme vzorec pro $\mathcal{A}(x_1,x_2,x_3)$ potřebovali znát.

10.27. Poznámka. V mnoha příkladech na lineární zobrazení se setkáváme se zobrazením do stejného lineárního prostoru. Bude tedy užitečné uvést následující definici.

10.28. Definice. Lineární zobrazení $\mathcal{A}\colon L \to L$ (tj. z lineárního prostoru do *téhož* lineárního prostoru) se nazývá *lineární transformace*. Nechť $\mathcal{A}\colon L \to L$ je lineární transformace, $\dim L =$

n. Matici $\mathcal{M}_{B,B}(\mathcal{A}) \in \mathbf{R}^{n,n}$ nazýváme *maticí transformace vzhledem k uspořádané bázi* (B). Ušetříme si tedy koktání: místo abychom mluvili o matici lineárního zobrazení vzhledem k bázím (B) a (B), říkáme stručněji matice transformace vzhledem k bázi (B).

10.29. Příklad. V lineárním prostoru U_O orientovaných úseček se společným počátkem O (viz příklad ??) jsou dány tři lineárně nezávislé vektory $\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3$. Uvažujme transformaci $\mathcal{A}\colon U_O \to U_O$, která každé orientované úsečce přiřadí její stín na rovině procházející vektory $\boldsymbol{b}_2, \boldsymbol{b}_3$, přitom světelné paprsky jsou rovnoběžné s vektorem $\boldsymbol{b}_1$. Taková transformace se nazývá *projekce*.

Zřejmě je $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ uspořádaná báze lineárního prostoru U_O. Najdeme matici $\mathcal{M}_{B,B}(\mathcal{A})$ transformace $\mathcal{A}$ vzhledem k uspořádané bázi (B).

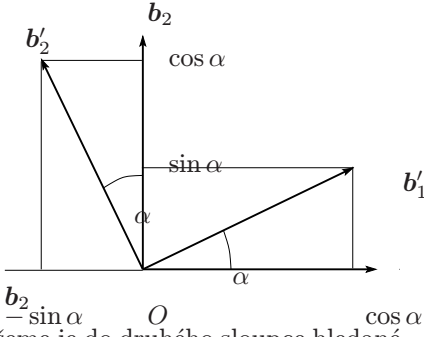
Platí $\mathcal{A}(\boldsymbol{b}_1) = \boldsymbol{o}$, $\mathcal{A}(\boldsymbol{b}_2) = \boldsymbol{b}_2$, $\mathcal{A}(\boldsymbol{b}_3) = \boldsymbol{b}_3$. Souřadnice těchto obrazů vzhledem k bázi (B) po řadě jsou $(0,0,0)$, $(0,1,0)$, $(0,0,1)$. Tyto souřadnice zapíšeme do sloupců hledané matice:

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \qquad \text{Protože platí:} \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ y \\ z \end{pmatrix},$$

má vektor $\boldsymbol{u} \in U_O$ se souřadnicemi (x, y, z) svůj stín, který má souřadnice $(0, y, z)$.

10.30. Příklad. V lineárním prostoru U_O orientovaných úseček s počátkem v bodě O (viz příklad ??) zvolme podprostor P dimenze 2 (vektory ležící ve společné rovině). V tomto prostoru P zvolme bázi $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2)$ tak, že vektory báze jsou na sebe kolmé a mají jednotkovou velikost (jako na obrázku níže). Transformaci, která otočí každý vzor o pevně zvolený úhel α označíme $\mathcal{R}_\alpha : P \to P$ a budeme jí říkat *rotace*. Najdeme matici $\mathcal{M}_{B,B}(\mathcal{R}_\alpha)$ této transformace vzhledem k bázi (B).

Na obrázku jsou kromě báze $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2)$ vyznačeny též obrazy báze $\mathcal{R}_\alpha(\boldsymbol{b}_1) = \boldsymbol{b}'_1$ a $\mathcal{R}_\alpha(\boldsymbol{b}_2) = \boldsymbol{b}'_2$, které jsou otočeny vzhledem ke svým vzorům o úhel α. Z vlastností funkcí kosinus a sinus plyne, že



$$\boldsymbol{b}'_1 = (\cos\alpha)\,\boldsymbol{b}_1 + (\sin\alpha)\,\boldsymbol{b}_2,$$

Z tohoto vztahu okamžitě vidíme souřadnice obrazu $\boldsymbol{b}'_1$ vzhledem k bázi (B). V souladu s větou ?? zapíšeme tyto souřadnice do prvního sloupce sestavované matice. Dále ze vztahu

$$\boldsymbol{b}'_2 = (-\sin\alpha)\,\boldsymbol{b}_1 + (\cos\alpha)\,\boldsymbol{b}_2$$

odhalíme souřadnice obrazu $\boldsymbol{b}'_2$ vzhledem k bázi (B) a zapíšeme je do druhého sloupce hledané matice. Dostáváme

$$\mathcal{M}_{B,B}(\mathcal{R}_\alpha) = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

Nechť vektor $\boldsymbol{u} \in P$ má souřadnice (x, y) vzhledem k bázi (B). Vypočítáme souřadnice vektoru, který vznikne otočením vektoru $\boldsymbol{u}$ o úhlel α. Použijeme větu ??.

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\cos\alpha - y\sin\alpha \\ x\sin\alpha + y\cos\alpha \end{pmatrix}.$$

Souřadnice otočeného vektoru vzhledem k bázi (B) tedy jsou (x', y'), kde

$$\begin{aligned} x' &= x\cos\alpha - y\sin\alpha, \\ y' &= x\sin\alpha + y\cos\alpha. \end{aligned}$$

10.31. Věta.* Nechť $\mathcal{A}\colon L_1 \to L_2$ je lineární zobrazení prostorů konečné dimenze, nechť $\mathbf{A}$ je jeho matice vzhledem k nějaké bázi (B) v L_1 a bázi (C) v L_2. Pak $\operatorname{hod}\mathcal{A} = \operatorname{hod}\mathbf{A}$.

Důkaz. Symboly $\mathcal{A}'$, $\mathcal{C}_B$ a $\mathcal{C}_C$ v tomto důkazu znamenají totéž co v definici ??. Díky větě ?? stačí ukázat, že $\operatorname{hod}\mathcal{A} = \operatorname{hod}\mathcal{A}'$, kde $\mathcal{A}' = \mathcal{C}_C \circ \mathcal{A} \circ \mathcal{C}_B^{-1}$, neboli $\mathcal{A} = \mathcal{C}_C^{-1} \circ \mathcal{A}' \circ \mathcal{C}_B$. Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je báze v L_1 a $(S_n) = (\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n)$ je standardní báze v $\mathbf{R}^n$. Platí $\boldsymbol{e}_i = \mathcal{C}_B(\boldsymbol{b}_i)$. Nyní spočítejme $\operatorname{hod}\mathcal{A}$:

$$\begin{aligned} \operatorname{hod}\mathcal{A} &= \dim\mathcal{A}(L_1) = \dim\mathcal{A}\big(\langle \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\rangle\big) = \dim\big\langle \mathcal{A}(\boldsymbol{b}_1), \mathcal{A}(\boldsymbol{b}_2), \ldots, \mathcal{A}(\boldsymbol{b}_n)\big\rangle = \\ &= \dim\big\langle \mathcal{C}_C^{-1} \circ \mathcal{A}' \circ \mathcal{C}_B(\boldsymbol{b}_1),\ \mathcal{C}_C^{-1} \circ \mathcal{A}' \circ \mathcal{C}_B(\boldsymbol{b}_2),\ \ldots,\ \mathcal{C}_C^{-1} \circ \mathcal{A}' \circ \mathcal{C}_B(\boldsymbol{b}_n)\big\rangle = \\ &= \dim\mathcal{C}_C^{-1}\big(\langle \mathcal{A}'(\boldsymbol{e}_1), \mathcal{A}'(\boldsymbol{e}_2), \ldots, \mathcal{A}'(\boldsymbol{e}_n)\rangle\big) \overset{\star}{=} \dim\big\langle \mathcal{A}'(\boldsymbol{e}_1), \mathcal{A}'(\boldsymbol{e}_2), \ldots, \mathcal{A}'(\boldsymbol{e}_n)\big\rangle = \\ &= \dim\mathcal{A}'\big(\langle \boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n\rangle\big) = \dim\mathcal{A}'(\mathbf{R}^n) = \operatorname{hod}\mathcal{A}' \end{aligned}$$

Rovnost označená hvězdičkou platí kvůli tomu, že $\mathcal{C}_C^{-1}$ je isomorfismus, takže zachovává dimenzi lineárních podprostorů.

10.32. Věta. Lineární transformace prostoru konečné dimenze je prostá právě tehdy, když má regulární matici.

Důkaz. Lineární transformace $\mathcal{A}\colon L \to L$ je prostá právě když má nulový defekt (viz větu ??). To platí právě tehdy, když $\operatorname{hod}\mathcal{A} = \operatorname{hod}\mathbf{A} = \dim L = n$ (viz věty ?? a ??). Matice $\mathbf{A} \in \mathbf{R}^{n,n}$ transformace $\mathcal{A}$ je regulární právě tehdy, když $\operatorname{hod}\mathbf{A} = n$ (viz větu ??).

10.33. Příklad. Určíme hodnost a defekt lineárního zobrazení $\mathcal{A}$ z příkladu ??.

Hodnost zobrazení $\mathcal{A}$ je rovna podle věty ?? hodnosti jeho matice. Tu jsme sestavili v příkladu ??. Matice zobrazení má hodnost 3, tedy i $\operatorname{hod}\mathcal{A} = 3$. Defekt zobrazení $\mathcal{A}$ spočítáme podle vzorce $\operatorname{def}\mathcal{A} + \operatorname{hod}\mathcal{A} = \dim L_1 = 4$, takže $\operatorname{def}\mathcal{A} = 1$.

10.34. Příklad. Určíme hodnost a defekt lineárního zobrazení $\mathcal{A}$ z příkladu ??.

Hodnost zobrazení $\mathcal{A}$ je rovna podle věty ?? hodnosti jeho matice. Tu jsme sestavili v příkladu ??. Matice zobrazení má hodnost 2, tedy i $\operatorname{hod}\mathcal{A} = 2$. Defekt zobrazení $\mathcal{A}$ spočítáme podle vzorce $\operatorname{def}\mathcal{A} + \operatorname{hod}\mathcal{A} = \dim L_1 = 3$, takže $\operatorname{def}\mathcal{A} = 1$.

Toto zobrazení tedy převede 3D vzor ($\dim L_1 = 3$) na 2D obraz ($\operatorname{hod}\mathcal{A} = 2$), tedy při tomto zobrazení ztrácíme informace z jedné dimenze ($\operatorname{def}\mathcal{A} = 1$). To vysvětluje, proč se

tomuto zobrazení říká projekce. S tímto slovem se jistě čtenář setkal v souvislosti s promítáním filmů.

10.35. Příklad. Protože matice z příkladů ?? a ?? jsou maticemi stejného lineárního zobrazení (jen vzhledem k různé bázi v L_1), mají hodnost rovnu hodnosti tohoto zobrazení. Tím je zaručeno, že tyto matice mají stejnou hodnost. Z výsledku příkadu ?? víme, že tyto matice mají hodnost 3.

10.36. Příklad. Matice rotace z příkladu ?? je regulární, protože $\det \mathcal{M}_{B,B}(\mathcal{R}_\alpha) = \cos^2 \alpha + \sin^2 \alpha = 1$. Podle věty ?? je tedy rotace prostá transformace.

10.37. Příklad. Budeme pracovat se stejným lineárním podprostorem P orientovaných úseček jako v příkladu ?? a zvolíme stejnou uspořádanou bázi (B). Zvolme dále čísla $a \in \mathbf{R}$, $b \in \mathbf{R}$. Popíšeme transformaci $\mathcal{S}_{a,b} : P \to P$, která má matici

$$\mathbf{A} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \tag{10.5}$$

vzhledem k bázi (B). Po použití věty ?? vidíme, že vektor $\boldsymbol{u} \in P$ se souřadnicemi (x, y) se zobrazí na vektor se souřadnicemi (ax, by). Co to geometricky znamená pro různé parametry a, b?

Při $a = 1$ a $b = 1$ zobrazení $\mathcal{S}$ ponechává vektor $\boldsymbol{u}$ beze změny. Takové transformaci říkáme *identita*.

V případě $a = -1$ a $b = 1$ zobrazení $\mathcal{S}$ transformuje vektor $\boldsymbol{u}$ na jeho osově souměrný protějšek podle osy, která prochází vektorem $\boldsymbol{b}_2$. V případě $a = 1$ a $b = -1$ zobrazení $\mathcal{S}$ transformuje vektor $\boldsymbol{u}$ na jeho osově souměrný protějšek podle osy, která prochází vektorem $\boldsymbol{b}_1$. Takové transformace se nazývají *osová souměrnost*.

V případě $a = -1$ a $b = -1$ zobrazení $\mathcal{S}$ zobrazí vektor $\boldsymbol{u}$ na vektor $-\boldsymbol{u}$ a této transformaci říkáme středová souměrnost (podle počátku O).

V případě $a = 0$ a $b = 1$ je zobrazení $\mathcal{S}$ projekcí na přímku, která prochází vektorem $\boldsymbol{b}_2$. V případě $a = 1$ a $b = 0$ je $\mathcal{S}$ projekcí na přímku, která prochází vektorem $\boldsymbol{b}_1$. V těchto případech se 2D vzor „promítá“ na 1D obraz, takže zde máme v množině vzorů i obrazů o jednu dimenzi méně než v příkladu ??. Je $\operatorname{hod} \mathcal{S} = 1$ a $\operatorname{def} \mathcal{S} = 1$.

V případě $a > 0$ a $b = 1$ je obraz a-krát deformován ve směru vektoru $\boldsymbol{b}_1$. V případě $a = 1$ a $b > 0$ je obraz b-krát deformován ve směru vektoru $\boldsymbol{b}_2$. V případě $a > 0$ a $b > 0$ je obraz deformován v obou směrech. Takové transformaci říkáme *změna měřítka*. Při $a = b$ této transformaci říkáme *stejnolehlost*.

Obecný případ $a \in \mathbf{R}$ a $b \in \mathbf{R}$ odpovídá transformaci změny měřítka případně složenou s osovou nebo středovou souměrností. Při $a = 0$ nebo $b = 0$ je $\mathcal{S}$ projekce. Při $a = 0$ i $b = 0$ je $\mathcal{S}$ zobrazení, které každému vektoru přiřadí nulový vektor. Defekt tohoto zobrazení je 2 a hodnost nula.

Zobrazení $\mathcal{S}_{a,b}: P \to P$ s maticí (10.5) budeme nadále říkat *změna měřítka*. Pod tímto pojmem budeme zahrnovat i všechny speciální případy zde vyjmenované.

10.38. Věta.* Nechť L_1 a L_2 jsou lineární prostory, $\dim L_1 = n$, $\dim L_2 = m$. Lineární prostor všech lineárních zobrazení z L_1 do L_2 je izomorfní s lineárním prostorem matic $\mathbf{R}^{m,n}$.

Důkaz (pro hloubavé čtenáře). Označme T lineární prostor všech lineárních zobrazení z L_1 do L_2. Zvolme nějakou uspořádanou bázi v L_1 a označme ji (B). Také označme (C) uspořádanou bázi v L_2. (viz též obrázek u definice ??). Ukážeme, že zobrazení $\mathcal{M}_{B,C}: T \to \mathbf{R}^{m,n}$, které přiřazuje zobrazením z T jejich matice vzhledem k bázím (B) a (C), je izomorfismus.

Obrazy zobrazení $\mathcal{M}_{B,C}$ jednoznačně existují pro všechna $\mathcal{A} \in T$, protože každému $\mathcal{A}$ je jednoznačně přiřazeno $\mathcal{A}' = \mathcal{C}_C \circ \mathcal{A} \circ \mathcal{C}_B^{-1}$ a každému takovému $\mathcal{A}': \mathbf{R}^n \to \mathbf{R}^m$ je jednoznačně přiřazena matice $\mathbf{A}$ díky větě ??.

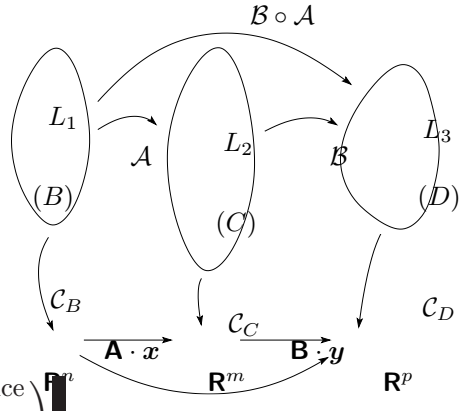
Zobrazení $\mathcal{M}_{B,C}$ je prosté a „na“ $\mathbf{R}^{m,n}$. To plyne z rovnosti (10.4), ve které vidíme, že matice $\mathbf{A}$ udává hodnoty zobrazení $\mathcal{A}$ na bázi (B). Podle věty ?? existuje jediné lineární zobrazení s takto určenými hodnotami na bázi.

Že je $\mathcal{M}_{B,C}$ lineární plyne z toho, že $\mathcal{M}_{B,C}(\mathcal{A})$ obsahuje ve sloupcích souřadnice obrazů báze (B) vzhledem k (C). Takže matice zobrazení $\mathcal{A}+\mathcal{B}$ je nutně součtem matic zobrazení $\mathcal{A}$ a $\mathcal{B}$ (obrazy báze se sčítají, jejich souřadnice rovněž). Podobné tvrzení platí pro α-násobek.

Zobrazení $\mathcal{M}_{B,C}: T \to \mathbf{R}^{m,n}$ je tedy prosté, na $\mathbf{R}^{m,n}$ a lineární. Je to tedy izomorfismus.

10.39. Poznámka. V důkazu předchozí věty jsme ukázali, že přechod od lineárního zobrazení k jeho matici je izomorfismus. To je důvod, proč často matematik napíše matici a myslí přitom na lineární zobrazení nebo naopak, pracuje s lineárním zobrazením a hledá k němu matici.

10.40. Věta.* Nechť L_1, L_2, L_3 jsou lineární prostory konečné dimenze, $\mathcal{A}\colon L_1 \to L_2$, $\mathcal{B}\colon L_2 \to L_3$ jsou lineární zobrazení. Nechť dále (B) je uspořádaná báze L_1, (C) je uspořádaná báze L_2 a (D) je uspořádaná báze L_3. Předpokládejme ještě, že $\mathcal{M}_{B,C}(\mathcal{A}) = \mathbf{A}$ je matice zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C) a konečně $\mathcal{M}_{C,D}(\mathcal{B}) = \mathbf{B}$ je matice zobrazení $\mathcal{B}$ vzhledem k bázím (C) a (D). Pak $\mathbf{B}\cdot\mathbf{A}$ je matice složeného zobrazení $\mathcal{B}\circ\mathcal{A}$ vzhledem k bázím (B) a (D).



Důkaz. Použijeme dvakrát za sebou větu ??. Pro každý vektor $\boldsymbol{u} \in L_1$ platí:

$$\mathbf{B}\cdot\mathbf{A}\cdot\begin{pmatrix}\text{souřadnice}\\ \text{vektoru}\\ \boldsymbol{u}\\ \text{vzhledem}\\ \text{k } (B)\end{pmatrix} = \mathbf{B}\cdot\begin{pmatrix}\text{souřadnice}\\ \text{vektoru}\\ \mathcal{A}(\boldsymbol{u})\\ \text{vzhledem}\\ \text{k } (C)\end{pmatrix} = \begin{pmatrix}\text{souřadnice}\\ \text{vektoru}\\ \mathcal{B}\big(\mathcal{A}(\boldsymbol{u})\big)\\ \text{vzhledem}\\ \text{k } (D)\end{pmatrix}$$

Platí $\mathcal{B}\big(\mathcal{A}(\boldsymbol{u})\big) = (\mathcal{B}\circ\mathcal{A})(\boldsymbol{u})$. Z věty ?? plyne, že $\mathbf{B}\cdot\mathbf{A}$ musí být maticí zobrazení $\mathcal{B}\circ\mathcal{A}$ vzhledem k bázím (B) a (D).

10.41. Poznámka. Větu ?? můžeme stručně zapsat takto:

$$\mathcal{M}_{B,D}(\mathcal{B}\circ\mathcal{A}) = \mathcal{M}_{C,D}(\mathcal{B})\cdot\mathcal{M}_{B,C}(\mathcal{A}) \tag{10.6}$$

10.42. Věta. Nechť L je lineární prostor konečné dimenze a (B) je jeho uspořádaná báze. Nechť $\mathcal{A}\colon L\to L$ je prostá lineární tranformace. Pak $\mathcal{A}$ je izomorfismus, tj. existuje inverzní transformace $\mathcal{A}^{-1}$ a platí

$$\mathcal{M}_{B,B}(\mathcal{A}^{-1}) = \big(\mathcal{M}_{B,B}(\mathcal{A})\big)^{-1}.$$

Důkaz. Protože $\mathcal{A}$ je prostá, je $\operatorname{def}\mathcal{A}=0$. Podle věty ?? je $\operatorname{def}\mathcal{A}+\operatorname{hod}\mathcal{A}=0+\operatorname{hod}\mathcal{A}=\dim L$. Je $\operatorname{hod}\mathcal{A}=n$ a věta ?? nám zaručí, že $\mathcal{A}(L)=L$. Takže transformace $\mathcal{A}$ je nejen prostá, ale i „na“ L, tedy je to izomorfismus. Symbolem $\mathcal{I}$ označme identické zobrazení na L. Pro $\mathcal{A}^{-1}$ platí $\mathcal{I}=\mathcal{A}^{-1}\circ\mathcal{A}$. Podle věty ?? tedy je

$$\mathcal{M}_{B,B}(\mathcal{A}^{-1})\cdot\mathcal{M}_{B,B}(\mathcal{A}) = \mathcal{M}_{B,B}(\mathcal{I}) = \mathbf{E}$$

Matice identity je jednotková matice $\mathbf{E}$. Matice $\mathcal{M}_{B,B}(\mathcal{A})$ je podle věty ?? regulární, takže můžeme maticí $\big(\mathcal{M}_{B,B}(\mathcal{A})\big)^{-1}$ vynásobit uvedenou rovnost zprava. Tím dostáváme dokazovaný vztah.

10.43. Příklad. Budeme pracovat v lineárním prostoru P s uspořádanou bází (B) jako v příkladu ??. Lineární transformace $\mathcal{A}\colon P \to P$ otočí vzor o stanovený úhel α a následně jej promítne na přímku procházející vektorem $\boldsymbol{b}_2$. Najdeme matici této transformace.

Platí $\mathcal{A} = \mathcal{S}_{0,1} \circ \mathcal{R}_\alpha$, kde $\mathcal{S}_{0,1}\colon P \to P$ je projekce a $\mathcal{R}_\alpha\colon P \to P$ je rotace o úhel α. Matice těchto transformací vzhledem k bázi (B) jsou:

$$\mathcal{M}_{B,B}(\mathcal{R}_\alpha) = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}, \qquad \mathcal{M}_{B,B}(\mathcal{S}_{0,1}) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Podle věty ?? je matice složeného zobrazení $\mathcal{A}$ rovna

$$\mathcal{M}_{B,B}(\mathcal{A}) = \mathcal{M}_{B,B}(\mathcal{S}_{0,1}) \cdot \mathcal{M}_{B,B}(\mathcal{R}_\alpha) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

Má-li vektor $\boldsymbol{u}$ souřadnice (x, y) vzhledem k (B), pak $\mathcal{A}(\boldsymbol{u})$ má vzhledem k (B) souřadnice (x', y'):

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ \sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ (\sin\alpha)\, x + (\cos\alpha)\, y \end{pmatrix}$$

Povšimneme si, že kdybychom zobrazení složili v opačném pořadí, tj. $\mathcal{R}_\alpha \circ \mathcal{S}_{0,1}$, dostaneme jiný výsledek. Stejně tak součin matic těchto zobrazení v opačném pořadí dává jiný výsledek.

10.44. Příklad. Budeme stále pracovat v lineárním prostoru P s uspořádanou bází (B) jako v příkladu ??. Nakreslíme v něm přímku p procházející počátkem, která svírá s vektorem $\boldsymbol{b}_1$ úhel α. Najdeme matici osové souměrnosti podle přímky p.

Osovou souměrnost podle p vytvoříme složením tří zobrazení: nejprve otočíme přímku p o úhel $-\alpha$. Její obraz tedy prochází vektorem $\boldsymbol{b}_1$. Dále provedeme osovou souměrnost podle přímky procházející vektorem $\boldsymbol{b}_1$ a nakonec otočíme obraz přímky na své místo otočením o úhel α. Matice jednotlivých transformací vzhledem k bázi (B) jsou

$$\mathcal{M}_{B,B}(\mathcal{R}_{-\alpha}) = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}, \quad \mathcal{M}_{B,B}(\mathcal{S}_{1,-1}) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathcal{M}_{B,B}(\mathcal{R}_{\alpha}) = \begin{pmatrix} \cos\alpha & -s \\ \sin\alpha & c \end{pmatrix}$$

Hledaná matice osové souměrnosti podle přímky p je součinem těchto matic ve správném pořadí:

$$\mathcal{M}_{B,B}(\mathcal{A}) = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} = \begin{pmatrix} \cos^2\alpha - \sin^2\alpha & 2\cos\alpha\sin \\ 2\cos\alpha\sin\alpha & -\cos^2\alpha + si \end{pmatrix}$$

Podle vzorečků o dvojnásobném úhlu můžeme výslednou matici přepsat do tvaru:

$$\mathcal{M}_{B,B}(\mathcal{A}) = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix}$$

Má-li vektor $\boldsymbol{u} \in P$ souřadnice (x, y) vzhledem k bázi (B), pak jeho osově souměrný obraz podle přímky p má vzhledem k bázi (B) souřadnice (x', y'):

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} (\cos 2\alpha)\, x + (\sin 2\alpha)\, y \\ (\sin 2\alpha)\, x - (\cos 2\alpha)\, y \end{pmatrix}$$

10.45. Definice.* Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ a $(C) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n)$ jsou dvě uspořádané báze lineárního prostoru L. Podle věty ?? existuje jediná lineární transformace $\mathcal{A}\colon L \to L$ taková, že $\mathcal{A}(\boldsymbol{b}_i) = \boldsymbol{c}_i$ pro všechna $i \in \{1, 2, \ldots, n\}$. Matici $\mathcal{M}_{B,B}(\mathcal{A})$ transformace $\mathcal{A}$ vzhledem k bázi (B) nazýváme *maticí přechodu od báze (B) k bázi (C)* a značíme ji $\mathbf{P}_{B\to C}$.

10.46. Věta.* Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ a $(C) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n)$ jsou dvě uspořádané báze lineárního prostoru L. Matice přechodu $\mathbf{P}_{B\to C}$ má následující vlastnosti:

(1) $\mathbf{P}_{B\to C}$ má v i-tém sloupci souřadnice vektoru $\boldsymbol{c}_i$ vzhledem k bázi (B) pro všechna $i \in \{1, 2, \ldots, n\}$,

(2) platí maticová rovnost $(\boldsymbol{c}_1\ \boldsymbol{c}_2\ \ldots\ \boldsymbol{c}_n) = (\boldsymbol{b}_1\ \boldsymbol{b}_2\ \ldots\ \boldsymbol{b}_n) \cdot \mathbf{P}_{B\to C}$,

(3) $\mathbf{P}_{B\to C} = \mathcal{M}_{C,B}(\mathcal{I})$, tj. $\mathbf{P}_{B\to C}$ je maticí identity vzhledem k bázím (C) a (B),

(4) pro každý vektor $\boldsymbol{u} \in L$ platí $\mathbf{P}_{B\to C} \cdot \mathcal{C}_C(\boldsymbol{u})^T = \mathcal{C}_B(\boldsymbol{u})^T$, neboli

$$\mathbf{P}_{B\to C} \cdot \begin{pmatrix} \text{souřadnice} \\ \text{vektoru} \\ \boldsymbol{u} \\ \text{vzhledem} \\ \text{k } (C) \end{pmatrix} = \begin{pmatrix} \text{souřadnice} \\ \text{vektoru} \\ \boldsymbol{u} \\ \text{vzhledem} \\ \text{k } (B) \end{pmatrix}.$$

Důkaz. (1) Podle věty ?? obsahuje matice $\mathbf{P}_{B\to C}$ ve sloupcích souřadnice obrazů $\mathcal{A}(\boldsymbol{b}_i) = \boldsymbol{c}_i$ vzhledem k bázi (B), kde $\mathcal{A}\colon L \to L$ je lineární transformace z definice ??.

(2) Rozepsáním součinu $(\boldsymbol{c}_1\ \boldsymbol{c}_2\ \dots\ \boldsymbol{c}_n) = (\boldsymbol{b}_1\ \boldsymbol{b}_2\ \dots\ \boldsymbol{b}_n) \cdot \mathbf{P}_{B\to C}$ po sloupcích matice $\mathbf{P}_{B\to C}$ shledáváme, že je tento součin ekvivalentní s (1).

(3) Vzorec (2) lze psát jako $\big(\mathcal{I}(\boldsymbol{c}_1)\ \mathcal{I}(\boldsymbol{c}_2)\ \dots\ \mathcal{I}(\boldsymbol{c}_n)\big) = (\boldsymbol{b}_1\ \boldsymbol{b}_2\ \dots\ \boldsymbol{b}_n) \cdot \mathbf{P}_{B\to C}$ a dívat se na něj úhlem pohledu vzorce (10.4), kde $\mathcal{A} = \mathcal{I}$, a kde jsou prohozeny báze (B) a (C).

(4) plyne z (3) a z věty ??.

10.47. Poznámka. Povšimneme si opačného pořadí bází ve vlastnostech (3) a (4) v předchozí větě. Vlastnost (4) říká, že matice přechodu od báze (B) k bázi (C) umožní počítat souřadnice vektoru vzhledem k bázi (B), pokud jeho souřadnice známe vzhledem k bázi (C). Je zde tedy opačný směr toku informace, než by vyplývalo z názvu matice. Název matice je odvozen z vlastnosti (2), tj. matice transformuje pomocí maticového násobení bázi (B) na bázi (C).

10.48. Poznámka. Všechny vlastnosti ve větě ?? jednoznačně určují matici přechodu $\mathbf{P}_{B\to c}$. Jinými slovy každá z nich by se dala použít jako definice pojmu matice přechodu. Je to tím, že každá podmínka vymezuje matici $\mathbf{P}_{B\to C}$ jednoznačně a ve větě ?? jsme dokázali, že tato jediná matice je maticí přechodu od báze (B) k bázi (C).

10.49. Věta.* Matice přechodu je regulární a platí
(1) $\mathbf{P}_{C\to B} = (\mathbf{P}_{B\to C})^{-1}$,
(2) $\mathbf{P}_{B\to C} \cdot \mathbf{P}_{C\to D} = \mathbf{P}_{B\to D}$.

Důkaz. $\mathbf{P}_{B\to C}$ je čtvercová matice, protože to je matice transformace. Protože obsahuje podle (1) věty ?? ve sloupcích souřadnice bázových vektorů, jsou tyto sloupce lineárně nezávislé. Matice je tedy podle věty ?? regulární.

(1) Vztah vyplyne například vynásobením rovnosti (2) ve větě ?? maticí $(\mathbf{P}_{B\to C})^{-1}$ zprava.

(2) Užitím vzorce (10.6) a vlastnosti (3) věty ?? dostáváme:

$$\mathbf{P}_{B\to C} \cdot \mathbf{P}_{C\to D} = \mathcal{M}_{C,B}(\mathcal{I}) \cdot \mathcal{M}_{D,C}(\mathcal{I}) = \mathcal{M}_{D,B}(\mathcal{I}) = \mathbf{P}_{B\to D}.$$

10.50. Algoritmus.* Odvodíme algoritmus na efektivní sestavení matice přechodu vzhledem k libovolným bázím. Pravda, vlastnost (1) věty ?? dává návod, jak matici přechodu sestavit. Ovšem někdy se stává, že se souřadnice vzhledem k bázi (B) obtížně hledají.

Najdeme v lineárním prostoru L nějakou bázi, vzhledem ke které se souřadnice dobře hledají a označíme ji (S). Báze (S) může být standardní báze v $\mathbf{R}^n$, báze $(1, x, x^2, x^3)$ v lineárním prostoru polynomů nejvýše třetího stupně, báze orientovaných úseček jednotkové velikosti a na sebe kolmých v lineárním prostoru U_O atd.

Nechť jsou dány báze (B) a (C) v lineárním prostoru L. Pro výpočet matice přechodu od báze (B) k bázi (C) použijeme vzorce z předchozí věty:

$$\mathbf{P}_{B\to C} = \mathbf{P}_{B\to S} \cdot \mathbf{P}_{S\to C} = (\mathbf{P}_{S\to B})^{-1} \cdot \mathbf{P}_{S\to C}.$$

Přitom matice na pravé straně rovnosti sestavíme snadno: do sloupců matice $\mathbf{P}_{S\to B}$ napíšeme souřadnice vektorů báze (B) vzhledem k (S) a do sloupců matice $\mathbf{P}_{S\to C}$ napíšeme souřadnice vektorů báze (C) vzhledem k (S).

Abychom si ještě ušetřili práci s výpočtem inverzní matice a následným maticovým násobením, použijeme větu ??, která říká $(\mathbf{A} \,|\, \mathbf{B}) \sim (\mathbf{E} \,|\, \mathbf{A}^{-1}\mathbf{B})$, neboli

$$(\mathbf{P}_{S\to B} \,|\, \mathbf{P}_{S\to C}) \;\sim\; (\mathbf{E} \,|\, \mathbf{P}_{S\to B}^{-1} \cdot \mathbf{P}_{S\to C}) = (\mathbf{E} \,|\, \mathbf{P}_{B\to C}).$$

Tím dostáváme následující algoritmus:

Zapišme do sloupců matice souřadnice báze (B) vzhledem k bázi (S) a vedle svislé čáry ještě souřanice báze (C) vzhledem k bázi (S). Po elmininaci, která převede levý blok matice na jednotkovou matici, dostáváme v pravém bloku $\mathbf{P}_{B\to C}$, neboli matici přechodu od (B) k (C).

10.51. Příklad. V lineárním prostoru polynomů nejvýše třetího stupně jsou dány tři uspořádané báze:

$$(B) = \big(x+1, x-1, (x+1)^2, (x+1)^3\big),$$
$$(C) = (1, x+1, x^2+2, x^3+3),$$
$$(S) = (x^3, x^2, x, 1)$$

Najdeme matici přechodu od (B) k (C). Je zřejmé, že souřadnice polynomu se nám dobře počítají vzhledem k bázi (S), takže zapíšeme-li do sloupců souřadnice vektorů z báze (B) vzhledem k (S), dostáváme okamžitě $\mathbf{P}_{S\to B}$. Podobně postupujeme u matice $\mathbf{P}_{S\to C}$:

$$\mathbf{P}_{S\to B} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 3 \\ 1 & 1 & 2 & 3 \\ 1 & -1 & 1 & 1 \end{pmatrix}, \qquad \mathbf{P}_{S\to C} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 2 & 3 \end{pmatrix}.$$

Pomocí algoritmu ?? najdeme $\mathbf{P}_{B\to C}$.

$$(\mathbf{P}_{S\to B} \,|\, \mathbf{P}_{S\to C}) = \left(\begin{array}{cccc|cccc} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 3 & 0 & 0 & 1 & 0 \\ 1 & 1 & 2 & 3 & 0 & 1 & 0 & 0 \\ 1 & -1 & 1 & 1 & 1 & 1 & 2 & 3 \end{array}\right) \sim \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1/2 & 1 & -1/2 & 4 \\ 0 & 1 & 0 & 0 & -1/2 & 0 & -3/2 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right) = (\mathbf{E} \,|\, \mathbf{P}_{B}$$

Báze (S), (B) a (C) vymezují v tomto příkladě tři souřadnicové systémy stejného lineárního prostoru. Vezmene nyní jeden vektor (polynom) p daný vzorcem $p(x) = 2x^3 + x^2 - 3x$. Zapíšeme postupně souřadnice tohoto polynomu ve všech třech souřadnicových sytémech.

Souřadnice polynomu p vzhledem k (S) odhalíme snadno: $\mathcal{C}_S(p) = (2, 1, -3, 0)$. Zkusíme nyní najít jeho souřadnice vzhledem k bázi (C). Podle vzorce (4) věty ?? k tomu potřebujeme matici $\mathbf{P}_{C\to S}$. Tu získáme jako inverzi k matici $\mathbf{P}_{S\to C}$:

$$\mathbf{P}_{C\to S} = (\mathbf{P}_{S\to C})^{-1} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 2 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} -3 & -2 & -1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Od souřadnic polynomu p vzhledem k bázi (S) k souřadnicím vzhledem k bázi (C) přejdeme pomocí maticového násobení maticí $\mathbf{P}_{C\to S}$:

$$\mathcal{C}_C(p)^T = \mathbf{P}_{C\to S} \cdot \mathcal{C}_S(p)^T = \begin{pmatrix} -3 & -2 & -1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 1 \\ -3 \\ 0 \end{pmatrix} = \begin{pmatrix} -5 \\ -3 \\ 1 \\ 2 \end{pmatrix}.$$

Od souřadnic polynomu p vzhledem k bázi (C) k souřadnicím vzhledem k bázi (B) přejdeme pomocí maticového násobení maticí $\mathbf{P}_{B\to C}$. Tu jsme spočítali pomocí algoritmu ??.

$$\mathcal{C}_B(p)^T = \mathbf{P}_{B\to C} \cdot \mathcal{C}_C(p)^T = \begin{pmatrix} 1/2 & 1 & -1/2 & 4 \\ -1/2 & 0 & -3/2 & -1 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -5 \\ -3 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \\ -5 \\ 2 \end{pmatrix}.$$

Od souřadnic polynomu p vzhledem k bázi (B) k souřadnicím vzhledem k bázi (S) přejdeme pomocí maticového násobení maticí $\mathbf{P}_{S\to B}$:

$$\mathcal{C}_S(p)^T = \mathbf{P}_{S\to B} \cdot \mathcal{C}_B(p)^T = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 3 \\ 1 & 1 & 2 & 3 \\ 1 & -1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -1 \\ -5 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ -3 \\ 0 \end{pmatrix}$$

a dostáváme souřadnice, které jsme měli na začátku. Šlo pouze o to procvičit si změny souřadnicového systému za použití maticového násobení. Výsledek můžeme srovnat s příkladem ??, ve kterém jsme počítali totéž, ale souřadnice jsme hledali jako řešení soustavy lineárních rovnic.

10.52. Příklad. V lineárním prostoru $\mathbf{R}^3$ jsou dány dvě uspořádané báze:

$$(B) = \big((1,1,1),(2,1,3),(1,0,4)\big), \qquad (C) = \big((3,2,1),(2,1,4),(4,3,2)\big).$$

Navrhneme algoritmus, který převádí souřadnice vektoru $\boldsymbol{u} \in \mathbf{R}^3$ vzhledem k bázi (B) na jeho souřadnice vzhledem k bázi (C). Dané souřanice vzhledem k bázi (B) označíme (x, y, z). Hlednané souřadnice vzhledem k bázi (C) označíme (x', y', z'). Pro přechod ze souřadnic vektoru vzhledem k bázi (B) k souřadnicím vzhledem k bázi (C) potřebujeme matici přechodu $\mathbf{P}_{C\to B}$. Tu vypočítáme pomocí algoritmu ??. Do výchozí matice zapisujeme do sloupců souřadnice báze (C) vzhledem ke standardní bázi a následně souřadnice báze (B) vzhledem ke standardní bázi. Tyto souřadnice jsou přímo složky jednotlivých vektorů.

$$(\mathbf{P}_{S\to C} \,|\, \mathbf{P}_{S\to B}) = \left(\begin{array}{ccc|ccc} 3 & 2 & 4 & 1 & 2 & 1 \\ 2 & 1 & 3 & 1 & 1 & 0 \\ 1 & 4 & 2 & 1 & 3 & 4 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -1 & 1/2 & 1/2 \\ 0 & 1 & 0 & 0 & 3/4 & 5/4 \\ 0 & 0 & 1 & 1 & -1/4 & -3/4 \end{array}\right) = (\mathbf{E} \,|\, \mathbf{P}_{C\to B}$$

Souřadnice vzhledem k bázi (C) získáme maticovým násobením

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \mathbf{P}_{C\to B} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -1 & 1/2 & 1/2 \\ 0 & 3/4 & 5/4 \\ 1 & -1/4 & -3/4 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -x + \frac{1}{2}y + \frac{1}{2}z \\ \frac{3}{4}y + \frac{5}{4}z \\ x - \frac{1}{4}y - \frac{3}{4}z \end{pmatrix},$$

takže $x' = -x + \frac{1}{2}y + \frac{1}{2}z,\ y' = \frac{3}{4}y + \frac{5}{4}z,\ z' = x - \frac{1}{4}y - \frac{3}{4}z.$

10.53. Věta.* Nechť $\mathcal{A}\colon L_1 \to L_2$ je lineární zobrazení lineárních prostorů konečné dimenze. Nechť (B) a (B') jsou dvě báze v L_1 a dále něchť (C) a (C') jsou dvě báze v L_2. Pak platí:
(1) $\mathcal{M}_{B,C}(\mathcal{A}) \cdot \mathbf{P}_{B\to B'} = \mathcal{M}_{B',C}(\mathcal{A})$,
(2) $\mathbf{P}_{C'\to C} \cdot \mathcal{M}_{B,C}(\mathcal{A}) = \mathcal{M}_{B,C'}(\mathcal{A})$,
(3) $\mathbf{P}_{C'\to C} \cdot \mathcal{M}_{B,C}(\mathcal{A}) \cdot \mathbf{P}_{B\to B'} = \mathcal{M}_{B',C'}(\mathcal{A})$.

Důkaz. Nechť $\mathcal{I}_1\colon L_1 \to L_1$ je identita na L_1 a $\mathcal{I}_2\colon L_2 \to L_2$ je identita na L_2. Platí $\mathcal{I}_2 \circ \mathcal{A} = \mathcal{A} = \mathcal{A} \circ \mathcal{I}_1$. V důkazu použijeme vzorec (10.6) a vlastnost (3) věty ?? pro matici přechodu.

(1) $\mathcal{M}_{B,C}(\mathcal{A}) \cdot \mathbf{P}_{B\to B'} = \mathcal{M}_{B,C}(\mathcal{A}) \cdot \mathcal{M}_{B',B}(\mathcal{I}_1) = \mathcal{M}_{B',C}(\mathcal{A} \circ \mathcal{I}_1) = \mathcal{M}_{B',C}(\mathcal{A})$,
(2) $\mathbf{P}_{C'\to C} \cdot \mathcal{M}_{B,C}(\mathcal{A}) = \mathcal{M}_{C,C'}(\mathcal{I}_2) \cdot \mathcal{M}_{B,C}(\mathcal{A}) = \mathcal{M}_{B,C'}(\mathcal{I}_2 \circ \mathcal{A}) = \mathcal{M}_{B,C'}(\mathcal{A})$,
(3) dokážeme postupným použitím (1) a (2).

10.54. Algoritmus. Podobně, jako v případě algoritmu ??, odvodíme algoritmus na nalezení matice zobrazení $\mathcal{A}\colon L_1 \to L_2$ vzhledem k libovolným bázím. Zvolíme si bázi (S) lineárního prostoru L_2, vzhledem ke které se souřadnice dobře hledají. Úkolem bude najít matici zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C).

Pro matici $\mathcal{M}_{B,C}(\mathcal{A})$ použijeme vzorec (2) věty ??:

$$\mathcal{M}_{B,C}(\mathcal{A}) = \mathbf{P}_{C\to S} \cdot \mathcal{M}_{B,S}(\mathcal{A}) = (\mathbf{P}_{S\to C})^{-1} \cdot \mathcal{M}_{B,S}(\mathcal{A}).$$

Matice na pravé straně této rovnice zapíšeme snadno: Matice $\mathcal{M}_{B,S}(\mathcal{A})$ obsahuje ve sloupcích souřadnice obrazů $\mathcal{A}(\boldsymbol{b}_i)$ vzhledem k (S) a matice $\mathbf{P}_{S\to C}$ má ve sloupcích souřadnice $\boldsymbol{c}_i$ vzhledem k (S).

Abychom si ještě ušetřili práci s výpočtem inverzní matice a následným maticovým násobením, použijeme větu ??, která říká $(\mathbf{A}\,|\,\mathbf{B}) \sim (\mathbf{E}\,|\,\mathbf{A}^{-1}\mathbf{B})$, neboli

$$\big(\mathbf{P}_{S\to C}\,|\,\mathcal{M}_{B,S}(\mathcal{A})\big) \sim \big(\mathbf{E}\,|\,\mathbf{P}_{S\to C}^{-1}\cdot\mathcal{M}_{B,S}(\mathcal{A})\big) = \big(\mathbf{E}\,|\,\mathcal{M}_{B,C}(\mathcal{A})\big).$$

Dostáváme následující algoritmus:

Do sloupců napíšeme pod sebe souřadnice vektorů $\boldsymbol{c}_i$ vzhledem k (S), vpravo od nich vedle svislé čáry napíšeme do sloupců souřadnice vektorů $\mathcal{A}(\boldsymbol{b}_i)$ vzhledem k (S). Pak matici eliminujeme tak, abychom v levé části dostali $\mathbf{E}$. V pravé části pak máme matici zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C).

10.55. Příklad. Je dáno lineární zobrazení $\mathcal{A}\colon L_1 \to L_2$, které derivuje polynomy, stejně jako v příkladu ??. Dále jsou dány báze:

$(B) = (1, x{+}1, x^2{+}2, x^3{+}3)$ v prostoru L_1, $\qquad (C) = (x^2{+}3, x{-}2, x^2{-}x)$ v prostoru L_2.

Najdeme $\mathcal{M}_{B,C}(\mathcal{A})$, tedy matici zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C). Použijeme k tomu algoritmus ??. Protože $\mathcal{A}$ derivuje polynomy, platí:

$$\mathcal{A}(1) = 0, \quad \mathcal{A}(x+1) = 1, \quad \mathcal{A}(x^2+2) = 2x, \quad \mathcal{A}(x^3+3) = 3x^2.$$

Souřadnice těchto obrazů vzhledem k bázi $(S) = (x^2, x, 1)$ zapíšeme do sloupců matice a tím dostáváme matici $\mathcal{M}_{B,S}(\mathcal{A})$. Matici $\mathbf{P}_{S\to C}$ sestavíme tak, že do sloupců zapíšeme souřadnice báze (C) vzhledem k bázi (S).

$$\left(\mathbf{P}_{S\to C} \,|\, \mathcal{M}_{B,S}(\mathcal{A})\right) = \left(\begin{array}{ccc|cccc} 1 & 0 & 1 & 0 & 0 & 0 & 3 \\ 0 & 1 & -1 & 0 & 0 & 2 & 0 \\ 3 & -2 & 0 & 0 & 1 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1/5 & 4/5 & 6/5 \\ 0 & 1 & 0 & -1/5 & 6/5 & 9/5 \\ 0 & 0 & 1 & -1/5 & -4/5 & 9/5 \end{array}\right) = (\mathbf{E} \,|\, \mathcal{M}$$

10.56. Příklad. Pokud jsou dány hodnoty lineárního zobrazení na bázi (B), ale není znám vzorec pro výpočet hodnoty v libovolném bodě, pak podle věty ?? lineární zobrazení $\mathcal{A}$ s danou vlastností existuje a je právě jedno. Můžeme okamžitě sestavit matici $\mathcal{M}_{B,S}(\mathcal{A})$. Pokud chceme najít vzorec pro toto zobrazení v libovolném bodě $\boldsymbol{x}$ a chceme pracovat se souřadnicemi $\boldsymbol{x}$ vzhledem k (S) (což je obvyklé), je potřeba na matici $\mathcal{M}_{B,S}(\mathcal{A})$ uplatnit přechod od báze (B) k (S), neboli použít vzorec (1) věty ??. Předvedeme si to na zobrazení $\mathcal{A}\colon \mathbf{R}^3 \to \mathbf{R}^4$ z příkladu ??. Tam je dána uspořádaná báze

$$(B) = \big((1,1,2), (1,2,2), (2,1,5)\big) \quad \text{v } \mathbf{R}^3$$

a obrazy zobrazení $\mathcal{A}$ na této bázi

$$\mathcal{A}(1,1,2) = (1,0,1,0), \quad \mathcal{A}(1,2,2) = (2,0,2,0), \quad \mathcal{A}(2,1,5) = (1,2,2,1).$$

V příkladu ?? jsme na základě těchto údajů sestavili matici $\mathcal{M}_{B,S_4}(\mathcal{A})$, kde (S_4) je standardní báze v $\mathbf{R}^4$. Nyní potřebujeme provést ještě přechod od (B) ke standarní bázi (S_3) v $\mathbf{R}^3$. K tomu použijeme vzorec (1) věty ??:

$$\mathcal{M}_{S_3,S_4}(\mathcal{A}) = \mathcal{M}_{B,S_4}(\mathcal{A}) \cdot \mathbf{P}_{B\to S_3} = \mathcal{M}_{B,S_4}(\mathcal{A}) \cdot (\mathbf{P}_{S_3\to B})^{-1}$$

Matice za posledním rovnítkem lze zapsat snadno. Ještě si můžeme ušetřit výpočet invernzí matice a následný maticový součin, pokud použijeme větu ??, která říká $(\mathbf{A}\,|\,\mathbf{B}) \sim (\mathbf{E}\,|\,\mathbf{A}^{-1}\mathbf{B})$. Bohužel, tentokrát máme součin v opačném pořadí, takže musíme přejít k transponovaným maticím:

$$\mathcal{M}_{S_3,S_4}(\mathcal{A})^T = (\mathbf{P}^T_{S_3\to B})^{-1}\cdot\mathcal{M}_{B,S_4}(\mathcal{A})^T, \quad \text{takže:} \quad \big(\mathbf{P}^T_{S_3\to B}\,|\,\mathcal{M}_{B,S_4}(\mathcal{A})^T\big) \sim \big(\mathbf{E}\,|\mathcal{M}_{S_3,S_4}(\mathcal{A})^T\big).$$

Z toho plyne algoritmus: tentokrát *do řádků* pod sebe napíšeme složky bázových vektorů z (B) a vpravo od nich vedle svislé čáry zapíšeme *do řádků* složky obrazů báze. Po eliminaci, kdy vlevo je jednotková matice, najdeme vpravo transponovanou matici $\mathcal{M}_{S_3,S_4}(\mathbf{A})$.

$$\left(\begin{array}{ccc|cccc} 1 & 1 & 2 & 1 & 0 & 1 & 0 \\ 1 & 2 & 2 & 2 & 0 & 2 & 0 \\ 2 & 1 & 5 & 1 & 2 & 2 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|cccc} 1 & 0 & 0 & 0 & -4 & -2 & -2 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 2 & 1 & 1 \end{array}\right) = \big(\mathbf{E}\,|\mathcal{M}_{S_3,S_4}(\mathcal{A})^T\big).$$

Náš výsledek se shoduje s výsledkem příkladu ??. Ovšem na rozdíl od postupu v příkladu ?? jsme nyní nemuseli počítat vzorec pro $\mathcal{A}(x_1, x_2, x_3)$. Naopak, výstup z právě odvozeného

algoritmu se dá použít k sestavení hledaného vzorce pro $\mathcal{A}(x_1, x_2, x_3)$, protože platí

$$\mathcal{A}(x_1, x_2, x_3)^T = \mathcal{M}_{S_3,S_4}(\mathcal{A}) \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

10.57. Příklad. Nechť $\mathcal{A}$ je transformace z definice matice přechodu ??, která zobrazí bázi (B) na bázi (C). Víme, že $\mathcal{M}_{B,B}(\mathcal{A}) = \mathbf{P}_{B\to C}$. Jak vypadá matice $\mathcal{M}_{C,C}(\mathcal{A})$?

Podle věty ?? je $\mathbf{P}_{C\to B}\mathcal{M}_{B,B}(\mathcal{A})\mathbf{P}_{B\to C} = \mathcal{M}_{C,C}(\mathcal{A})$. Takže $\mathcal{M}_{C,C}(\mathcal{A}) = \mathbf{P}_{C\to B}\mathbf{P}_{B\to C}\mathbf{P}_{B\to C}$. Matice přechodu $\mathbf{P}_{B\to C}$ je tedy rovna nejenom $\mathcal{M}_{B,B}(\mathcal{A})$, ale také $\mathcal{M}_{C,C}(\mathcal{A})$.

10.58. Shrnutí. Lineární zobrazení z L_1 do L_2 lze mezi sebou sčítat a lze je násobit konstantou, přičemž tato lineární zobrazení s uvedenými operacemi tvoří lineární prostor /??, ??/.

Jsou-li dány hodnoty na bázi, existuje právě jedno lineární zobrazení, které má tyto hodnoty /??/.

Nechť L_1 má konečnou uspořádanou bázi (B) a L_2 má konečnou uspořádanou bázi (C). Každé lineární zobrazení $\mathcal{A}\colon L_1 \to L_2$ lze jednoznačně reprezentovat maticí $\mathbf{A}$ takovou, že platí $\mathbf{A} \cdot \boldsymbol{x} = \boldsymbol{y}$, kde $\boldsymbol{x}$ jsou souřadnice vzoru vzhledem k bázi (B) a $\boldsymbol{y}$ jsou souřadnice obrazu vzhledem k bázi (C). Tuto matici nazýváme maticí zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C) /??/.

Pro matici $\mathbf{A}$ zobrazení $\mathcal{A}$ platí, že ve sloupcích obsahuje souřadnice obrazů báze (B) vzhledem k bázi (C) /??/. Totéž lze vyjádřit maticovým násobením /??/.

Hodnost zobrazení $\mathcal{A}$ je rovna hodnosti jeho matice $\mathbf{A}$ /??, ??/. Souřadnice všech vektorů jádra zobrazení jsou množinou řešení homogenní soustavy rovnic $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$.

Přiřazení, které lineárnímu zobrazení přidělí jeho matici vzhledem k pevně zvoleným bázím, je izomorfismus /důkaz věty ??/.

Matice složeného zobrazení $\mathcal{B}\circ\mathcal{A}$ je rovna součinu jejich matic $\mathbf{B}\cdot\mathbf{A}$ ve stejném pořadí /??/. Matice inverzní transformace je rovna inverzní matici původní tansformace /??/.

Matice přechodu $\mathbf{P}_{B\to C}$ od báze (B) k bázi (C) je maticí transformace, která zobrazí $\boldsymbol{b}_i$ z báze (B) na $\boldsymbol{c}_i$ z báze (C) /??/. Obsahuje ve sloupcích souřadnice vektorů $\boldsymbol{c}_i$ vzhledem k bázi (B) a je rovna matici identity vzhledem k bázím (C) a (B) /??/. Matice $\mathbf{P}_{B\to C}$ umožní transformovat souřadnice vektoru $\boldsymbol{x}$ vzhledem k bázi (C) na souřadnice téhož vektoru vzhledem k bázi (B) /??/. Pozor: báze jsou zde v opačném pořadí.

Platí $\mathbf{P}_{B\to C}\cdot\mathbf{P}_{C\to D} = \mathbf{P}_{B\to D}$ a $\mathbf{P}_{B\to C} = (\mathbf{P}_{C\to B})^{-1}$ /??/.

Ve větě ?? jsme si uvědomili, jak se změní matice zobrazení, pohneme-li první nebo druhou bází. Je potřeba matici zobrazení vynásobit z příslušné strany příslušnými maticemi přechodu.

V odstavcích ?? a ?? jsme odvodili algoritmy na sestavení matice přechodu a matice zobrazení vzhledem k libovolným bázím, tj. i bázím, vzhledem k nimž se souřadnice vektorů počítají obtížněji.

11. Afinní transformace, matice v homogenních souřadnicích

11.1. Poznámka. V ?? kapitole jsme se setkali s maticemi transformací otočení /??/ a změny měřítka /??/. Do této skupiny tranformací řadíme ještě transformaci posunutí, která ale není lineární, protože nulový vektor „posune“ na nenulový vektor, což způsobně vychované lineární zobrazení kvůli větě ?? nedělá. Složením transformace posunutí s lineární transformací dostáváme tzv. *afinní transformaci*.

Afinní transformace tedy nemá obecně svoji matici. V následujícím textu ukážeme, že při použití speciálních souřadnic (tzv. *homogenních souřadnic*) je možné sestavit i matice všech afinních transformací a pracovat s nimi stejně jako s maticemi lineárních transformací. Tyto matice je možné v případě složené afinní transformace mezi sebou násobit. To má praktické využití například při programování transformací v počítačové grafice.

11.2. Poznámka. Nejprve si upřesníme vlastnosti geometrického prostoru, ve kterém budeme uvedené transformace uplatňovat. Tento prostor nazveme *afinní*. V něm budeme rozlišovat objekty dvou typů: *body* a *vektory*. Množinu všech bodů budeme značit $\mathbf{X}$. Do exaktního zavedení množiny $\mathbf{X}$ se nebudeme pouštět, stačí snad intuitivní chápání pojmu bod.

Vektor je určen orientovanou úsečkou, která je vymezena dvěma body z $\mathbf{X}$: počátečním a koncovým. Na rozdíl od lineárního prostoru U_O z příkladu ?? není nutné, aby orientovaná úsečka začínala v počátku. Navíc považujeme dvě orientované úsečky za reprezentanty stejného vektoru, pokud jsou rovnoběžné, stejně velké a stejně orientované. Součet dvou vektorů

provedeme jako v lineárním prostoru U_O, když si narýsujeme jejich orientované úsečky tak, aby začínaly ve společném bodě a doplníme na rovnoběžník. Násobek vektoru konstantou provedeme také obdobně jako v lineárním prostoru U_O. Množinu všech takových vektorů značíme V. Je zřejmé, že společně s uvedenými operacemi sčítání vektorů a násobení vektoru konstantou tvoří tato množina vektorů lineární prostor. Argumentuje se analogicky, jak v případě lineárního prostoru orientovaných úseček U_O v příkladu ??.

Dále zavedeme nové sčítání bodu $P \in \mathbf{X}$ s vektorem $\boldsymbol{u} \in V$ takto: součet $P+\boldsymbol{u}$ je koncový bod orientované úsečky vektoru $\boldsymbol{u}$, pokud její počáteční bod umístíme do bodu P.

11.3. Definice.* *Afinní prostor* je množina bodů $\mathbf{X}$ společně s lineárním prostorem vektorů V. Zapisujeme jej jako dvojici $(\mathbf{X}, V)$.

Kromě operací $+\colon V \times V \to V$ a $\cdot\colon \mathbf{R} \times V \to V$ splňující axiomy linearity (1) až (7) definice ?? je zavedena ještě operace $+\colon \mathbf{X} \times V \to \mathbf{X}$ s vlastnostmi:

(1) $P + \boldsymbol{o} = P$ pro všechny body $P \in \mathbf{X}$ ($\boldsymbol{o} \in V$ je nulový vektor),
(2) $(P + \boldsymbol{u}) + \boldsymbol{v} = P + (\boldsymbol{u} + \boldsymbol{v})$ pro všechny body $P \in \mathbf{X}$ a vektory $\boldsymbol{u} \in V$, $\boldsymbol{v} \in V$,
(3) pro všechny body $P \in \mathbf{X}$, $Q \in \mathbf{X}$ existuje právě jeden vektor $\boldsymbol{u} \in V$ tak, že $P = Q + \boldsymbol{u}$

11.4. Poznámka. Definice afinního prostoru je zavedena pomocí axiomů nové operace, jak je v algebře obvyklé. Nemusíme se tedy obtěžovat přesným vymezením pojmů bod z množiny

$\mathbf{X}$ a vektor z množiny V. Také nemusíme vědět, jak konkrétně pracuje operace „bod plus vektor“. Stačí, že tato operace splňuje uvedené axiomy.

Z axiomů plyne, že „vektorů je stejný počet jako bodů“. Přesněji, lze najít prosté zobrazení z množiny bodů na množinu vektorů. Stačí zvolit jeden bod $Q \in \mathbf{X}$ a dále pro všechna $P \in \mathbf{X}$ existuje podle axiomu (3) jediný vektor $\boldsymbol{u} \in V$. Tím je určeno prosté zobrazení z množiny bodů do množiny vektorů. Že je toto zobrazení „na“ plyne z toho, že ke každému vektoru $\boldsymbol{u} \in V$ lze zpětně sestrojit bod $P = Q + \boldsymbol{u}$.

V dalším textu si vystačíme s představou geometrického prostoru s intuitivním pojetím bodů a vektorů podle poznámky ??. Ukážeme, že tato představa je v souladu s definicí ??. Tj. ověříme platnost axiomů pro operaci sčítání bodu P s vektorem $\boldsymbol{u}$ zavedenou geometricky: $P + \boldsymbol{u}$ je koncový bod orientované úsečky vektoru $\boldsymbol{u}$, která začíná v bodě P.

Axiom (1): Vektor $\boldsymbol{o}$ má koncový bod ve stejném místě jako počáteční. Takže operace $P + \boldsymbol{o}$ bod P nezmění.

Axiom (2): Narýsujeme od bodu P orientovanou úsečku vektoru $\boldsymbol{u}$ a od koncového bodu této úsečky narýsujeme druhou orientovanou úsečku vektoru $\boldsymbol{v}$. Protože tyto dvě orientované úsečky vymezují „sčítací rovnoběžník“ pro výpočet $\boldsymbol{u} + \boldsymbol{v}$, je zřejmé, že $(P + \boldsymbol{u}) + \boldsymbol{v} = P + (\boldsymbol{u} + \boldsymbol{v})$.

Axiom (3): Vektor $\boldsymbol{u}$ je určený orientovanou úsečkou začínající v bodě Q a končící v bodě P. Tento vektor budeme značit $P - Q$ nebo $\overrightarrow{QP}$.

11.5. Poznámka. Lapidární shrnutí: v afinním prostoru používáme následující operace:

$$\begin{aligned} \text{vektor} + \text{vektor} &= \text{vektor},\\ \text{konstanta} \cdot \text{vektor} &= \text{vektor},\\ \text{bod} + \text{vektor} &= \text{bod},\\ \text{bod} - \text{bod} &= \text{vektor},\\ \text{bod} + \text{bod} &\ldots \textit{nemá smysl}. \end{aligned}$$

s vlastnostmi (1) až (7) z definice ?? a s vlastnostmi (1) až (3) z definice ??.

11.6. Definice. *Souřadnicový systém* v afinním prostoru $(\mathbf{X}, V)$ zavedeme tak, že zvolíme nějakou uspořádanou bázi (B) lineárního prostoru V a zvolíme bod $O \in \mathbf{X}$, kterému budeme říkat *počátek*. Souřadnicový systém budeme značit (O, B).

Souřadnice vektoru $\boldsymbol{u} \in V$ vzhledem k systému (O, B) jsou souřadnice vektoru $\boldsymbol{u}$ vzhledem k uspořádané bázi (B).

Souřadnice bodu $P \in \mathbf{X}$ vzhledem k systému (O, B) jsou souřadnice vektoru $P - O$ vzhledem k uspořádané bázi (B). Vektor $P - O$ se nazývá *radiusvektor bodu P*.

11.7. Definice. *Dimenze afinního prostoru* $(\mathbf{X}, V)$ je rovna dimenzi lineárního prostoru V. Typicky používáme afinní prostory dimenze 2 (rovina) nebo dimenze 3 (naše geometrické vnímání světa).

11.8. Věta. Nechť $(\mathbf{X}, V)$ je afinní prostor, nechť dále (O, B) je jeho souřadnicový systém. Nechť $\boldsymbol{u} \in V$, $\boldsymbol{v} \in V$ $\alpha \in \mathbf{R}$, $P \in \mathbf{X}$, $Q \in \mathbf{X}$. Symbolem $\mathcal{C}(.)$ značíme souřadnice bodu nebo vektoru vzhledem k (O, B). Platí

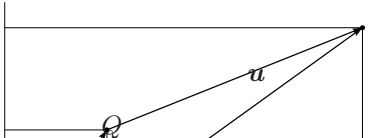
$$(1)\ \mathcal{C}(\boldsymbol{u} + \boldsymbol{v}) = \mathcal{C}(\boldsymbol{u}) + \mathcal{C}(\boldsymbol{v})$$
$$(2)\ \mathcal{C}(\alpha \cdot \boldsymbol{u}) = \alpha \cdot \mathcal{C}(\boldsymbol{u})$$
$$(3)\ \mathcal{C}(Q + \boldsymbol{u}) = \mathcal{C}(Q) + \mathcal{C}(\boldsymbol{u})$$
$$(4)\ \mathcal{C}(P - Q) = \mathcal{C}(P) - \mathcal{C}(Q)$$

Důkaz. (1) a (2) plyne z toho že V je lineární prostor a $\mathcal{C}$ značí souřadnice vektoru vzhledem k uspořádané bázi (B). Zobrazení $\mathcal{C}$ je na množině V podle věty ?? lineární.

(3) Radiusvektor bodu $Q+\boldsymbol{u}$ je součtem radiusvektoru bodu Q s vektorem $\boldsymbol{u}$. Souřadnice bodů jsou definovány jako souřadnice jejich radiusvektorů. Na V je podle věty ?? zobrazení $\mathcal{C}$ lineární.

(4) Vektor $P-Q$ je výsledkem operace „radiusvektor bodu P minus radiusvektor bodu Q“. Další argumentace je stejná jako v důkazu (3).

11.9. Příklad. Na obrázku jsme vyznačili souřadnicový systém (O, B) afinního prostoru dimenze 2. Vektory uspořádané báze $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2)$ jsou stejné



velikosti a na sebe kolmé. To není nutné, ale je to praktické.

Na obrázku jsou radiusvektory bodů $P \in \mathbf{X}$ a $Q \in \mathbf{X}$, takže jsme schopni určit souřadnice bodů: $\mathcal{C}(P) = (7,5)$ a $\mathcal{C}(Q) = (2,3)$. Dále je vyznačena orientovaná úsečka vektoru $\boldsymbol{u} = P - Q$. Vektor $\boldsymbol{u}$ určený touto úsečkou má podle věty ?? souřadnice rovny rozdílu souřadnic bodů:

$$\mathcal{C}(\boldsymbol{u}) = \mathcal{C}(P) - \mathcal{C}(Q) = (7,5) - (2,3) = (5,2).$$

Na obrázku je u dvou různých orientovaných úseček připsáno stejné písmeno $\boldsymbol{u}$, protože tyto úsečky jsou rovnoběžné, stejně velké a stejně orientované. Považujeme je za reprezentanty stejného vektoru $\boldsymbol{u}$.

11.10. Definice.* Nechť $(\mathbf{X}, V)$ je afinní prostor dimenze n a (O, B) je jeho souřadnicový systém.

Homogenní souřadnice bodu $P \in \mathbf{X}$ jsou uspořádaná $(n+1)$-tice, která v prvních n složkách obsahuje souřadnice bodu P vzhledem k (O, B) a v poslední složce obsahuje jedničku.

Homogenní souřadnice vektoru $\boldsymbol{u} \in V$ jsou uspořádaná $(n+1)$-tice, která v prvních n složkách obsahuje souřadnice vektoru $\boldsymbol{u}$ vzhledem k (O, B) a v poslední složce obsahuje nulu.

Upozornění: rozšířenou verzi definice homogenních souřadnic bodu najde čtenář v odstavci ??.

11.11. Příklad. Vraťme se k bodům P a Q v příkladu ??. Homogenní souřadnice bodu P jsou $(7, 5, 1)$, homogenní souřadnice bodu Q jsou $(2, 3, 1)$. Homogenní souřadnice vektoru $\boldsymbol{u} = P - Q$ jsou $(5, 2, 0)$.

11.12. Věta.* Vlastnosti (1) až (4) věty ?? jsou splněny i v případě, že $\mathcal{C}(.)$ značí homogenní souřadnice.

Důkaz. V případě lineárních kombinací vektorů zůstává v poslední složce souřadnic nula. Při součtu bodu s vektorem je v poslední složce souřadnic odehrává výpočet $1 + 0 = 1$, tedy dostáváme homogenní souřadnice bodu. Při odečítání bodů se v poslední složce souřadnic odečítají jedničky a vzniká nula, dostáváme tedy homogenní souřadnice vektoru.

11.13. Definice.* Nechť $(\mathbf{X}, V)$ je afinní prostor dimenze n a (O, B) jeho souřadnicový systém. Říkáme, že *transformace* $\mathcal{A} : \mathbf{X} \to \mathbf{X}$ *má matici* $\mathbf{A} \in \mathbf{R}^{n+1,n+1}$ *v homogeních souřadnicích vzhledem k* (O, B), pokud pro každý bod $P \in \mathbf{X}$ jsou homogenní souřadnice obrazu $\mathcal{A}(P)$ rovny sloupcovému vektoru $\mathbf{A} \cdot \boldsymbol{x}$, kde $\boldsymbol{x}$ jsou homogenní souřadnice bodu P. Jinak řečeno, pro každý

bod $P \in \mathbf{X}$ je

$$\mathbf{A} \cdot \begin{pmatrix} \text{homogenní} \\ \text{souřadnice} \\ \text{bodu } P \\ \text{vzhledem} \\ \text{k } (O,B) \end{pmatrix} = \begin{pmatrix} \text{homogenní} \\ \text{souřadnice} \\ \text{bodu } \mathcal{A}(P) \\ \text{vzhledem} \\ \text{k } (O,B) \end{pmatrix}$$

11.14. Poznámka. Nechť transformace $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$ má matici $\mathbf{A}$. Jak musí taková matice vypadat? Je-li $\boldsymbol{x}$ vektor homogenních souřadnic bodu, pak musí $\mathbf{A} \cdot \boldsymbol{x}$ být také vektor homogenních souřadnic bodu. Neboli jednička v poslední složce vektoru $\boldsymbol{x}$ musí zůstat zachována i po maticovém násobení. Z vlastností maticového náspobení vyplývá, že daný požadavek splňují všechny matice $\mathbf{A} \in \mathbf{R}^{n+1,n+1}$, které je možné do bloků rozepsat následovně:

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}' & \boldsymbol{t} \\ \boldsymbol{o} & 1 \end{pmatrix}, \tag{11.1}$$

kde $\mathbf{A}' \in \mathbf{R}^{n,n}$ je libovolná matice, $\boldsymbol{t} \in \mathbf{R}^{n,1}$ je libovolný sloupcový vektor, $\boldsymbol{o} \in \mathbf{R}^{1,n}$ je nulový vektor a vpravo dole je jednička. Jinými slovy je to matice, která má v posledním řádku nuly s výjimkou posledního prvku, který je roven jedné.

Nechť bod P má vzhledem k (O, B) souřadnice $\boldsymbol{p} \in \mathbf{R}^n$, takže jeho homogenní souřadnice jsou $(\boldsymbol{p}, 1)$. Pak platí:

$$\mathbf{A} \cdot \begin{pmatrix} \boldsymbol{p}^T \\ 1 \end{pmatrix} = \begin{pmatrix} \mathbf{A}' & \boldsymbol{t} \\ \boldsymbol{o} & 1 \end{pmatrix} \cdot \begin{pmatrix} \boldsymbol{p}^T \\ 1 \end{pmatrix} = \begin{pmatrix} \mathbf{A}'\boldsymbol{p}^T + \boldsymbol{t} \\ 1 \end{pmatrix}.$$

Z maticového násobení snadno plyne, že součin dvou matic typu (11.1) je matice typu (11.1). Tento součin je maticí odpovídajícího složeného zobrazení, jak ukážeme ve větě ??.

11.15. Příklad. V afinním prostoru dimenze 2 jsou matice transformací v homogenních souřadnicích tvaru:

$$\begin{pmatrix} a & b & c \\ d & e & f \\ 0 & 0 & 1 \end{pmatrix}, \qquad \text{tj.} \quad \begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = \begin{pmatrix} a & b & c \\ d & e & f \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} ax + by + c \\ dx + ey + f \\ 1 \end{pmatrix}.$$

Transformace v 2D prostoru jsou tedy určeny maticemi se šesti parametry a až f.

11.16. Příklad. V afinním prostoru dimenze 3 jsou matice transformací v homogenních souřadnicích tvaru:

$$\begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \text{tj.} \quad \begin{pmatrix} x' \\ y' \\ z' \\ 1 \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \\ 1 \end{pmatrix} = \begin{pmatrix} ax + by + cz + d \\ ex + fy + gz + h \\ ix + jy + kz + l \\ 1 \end{pmatrix}.$$

Transformace v 3D prostoru jsou tedy určeny maticemi s dvanácti parametry a až l.

11.17. Věta.* Nechť $(\mathbf{X}, V)$ je afinní prostor dimenze n a nechť (O, B) je jeho souřadnicový systém. Nechť transformace $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$ má matici $\mathbf{A}$ v homogenních souřadnicích vzhledem k (O, B) a transformace $\mathcal{B}\colon \mathbf{X} \to \mathbf{X}$ má matici $\mathbf{B}$ v homogenních souřadnicích vzhledem k (O, B). Pak složené zobrazení $\mathcal{B} \circ \mathcal{A}$ má matici $\mathbf{B} \cdot \mathbf{A}$ v homogenních souřadnicích vzhledem k (O, B).

Důkaz. Věta se dokáže stejně jako věta ??. Pouze místo slov „souřadnice vektoru vzhledem k bázi“ v důkazu používáme slova „homogenní souřadnice bodu vzhledem k (O, B)“.

11.18. Příklad. Uvedeme matice elementárních transformací v afinním prostoru $(\mathbf{X}, V)$ dimenze 2.

Změna měřítka a-krát ve směru první souřadnice a b-krát ve směru druhé má matici

$$\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{protože} \quad \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} a\,x \\ b\,y \\ 1 \end{pmatrix}.$$

Změna měřítka tansformuje vektory stejně jako body. Tento typ transformace byl podrobně diskutován v příkladu ??.

Rotace o úhel α kolem počátku má matici

$$\begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{protože} \quad \begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} x\,\cos\alpha - y\,\sin\alpha \\ x\,\sin\alpha + y\,\cos\alpha \\ 1 \end{pmatrix}.$$

Rotace transformuje vektory stejně jako body. Matice tohoto typu transformace byla odvozena v příkladu ??. Doplňujícím předpokladem pro tuto matici je souřadnicový systém s bází vektorů, které jsou na sebe kolmé a mají stejnou velikost.

Posunutí o vektor se souřadnicemi (t_x, t_y) má matici

$$\begin{pmatrix} 1 & 0 & t_x \\ 0 & 1 & t_y \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{protože} \quad \begin{pmatrix} 1 & 0 & t_x \\ 0 & 1 & t_y \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} x + t_x \\ y + t_y \\ 1 \end{pmatrix}.$$

Tato transformace posunuje jenom body, vektory nechává nezměněny.

Další transformace v afinním prostoru $(\mathbf{X}, V)$ vznikají jako skládání těchto elementárních trnasformací. Složené zobrazení má podle věty ?? matici rovnu součinu matic jednotlivých zobrazení.

11.19. Příklad. V afinním prostoru dimenze 2 najdeme matici $\mathbf{A}$ v homogenních souřadnicích takové transformace, která otáčí vzor kolem bodu se souřadnicemi $(2, 3)$ o úhel α. Tato

transformace je složením tří transformací: nejprve posune bod $(2,3)$ do počátku, pak otočí obraz kolem počátku o úhel α a nakonec posune počátek zpět do bodu $(2,3)$. Matice transformace je součinem matic transformací, ze kterých je složena, přitom nejdříve aplikovaná transformace má svou matici nejvíce vpravo (viz větu ??).

$$\mathbf{A} = \Big(\text{matice posunutí o } (2,3)\Big)\cdot\Big(\text{matice rotace o úhel } \alpha\Big)\cdot\Big(\text{matice posunutí o } (-2,-3)\Big) =$$

$$= \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}\cdot\begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix}\cdot\begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha & -2\cos\alpha + 3\sin\alpha - \\ \sin\alpha & \cos\alpha & -2\sin\alpha - 3\cos\alpha - \\ 0 & 0 & 1 \end{pmatrix}$$

11.20. Poznámka. V dalším textu ukážeme, že všechny transformace $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$, které mají matici v homogenních souřadnicích, jsou tzv. *afinní transformace* a dále dokážeme, že všechny afinní transformace mají matici v homogenních souřadnicích.

11.21. Definice.* Nechť $(\mathbf{X}, V)$ je afinní prostor. Transformace $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$ se nazývá *afinní transformace* (krátce *afinita*), pokud existuje lineární transformace $\mathcal{A}'\colon V \to V$ tak, že pro každý bod $P \in \mathbf{X}$ a pro každý vektor $\boldsymbol{u} \in V$ platí

$$\mathcal{A}(P + \boldsymbol{u}) = \mathcal{A}(P) + \mathcal{A}'(\boldsymbol{u}).$$

11.22. Věta.* Nechť $(\mathbf{X}, V)$ je afinní prostor dimenze n a $(O, B) = (O, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ je jeho souřadnicový systém. Pak afinní zobrazení $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$ je jednoznačně určeno svými obrazy v bodech O a $O + \boldsymbol{b}_i$ pro $i \in \{1, \ldots, n\}$.

Důkaz. Protože $\mathcal{A}$ je afinní, existuje lineární zobrazení $\mathcal{A}'\colon V \to V$, pro které platí

$$\mathcal{A}(O + \boldsymbol{b}_i) = \mathcal{A}(O) + \mathcal{A}'(\boldsymbol{b}_i).$$

Známe-li hodnoty $\mathcal{A}(O + \boldsymbol{b}_i)$ a $\mathcal{A}(O)$, pak jsou tímto vzorcem určeny i hodnoty $\mathcal{A}'(\boldsymbol{b}_i)$ pro všechny bázové vektory $\boldsymbol{b}_i$. Lineární zobrazení $\mathcal{A}'$ je podle věty ?? těmito hodnotami jednoznačně určeno. Hodnota zobrazení $\mathcal{A}$ v každém bodě $P \in \mathbf{X}$ je pak jednoznačně určena ze vztahu

$$\mathcal{A}(P) = \mathcal{A}\big(O + (P - O)\big) = \mathcal{A}(O) + \mathcal{A}'(P - O).$$

11.23. Věta. Nechť $(\mathbf{X}, V)$ je afinní prostor dimenze n a (O, B) je jeho souřadnicový systém. Pak každá transformace $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$, která má matici $\mathbf{A}$ v homogenních souřadnicích vzhledem k (O, B), je afinní transformace.

Důkaz. Nechť $\mathbf{A}$ je matice zobrazení $\mathcal{A}$ v homogenních souřadnicích. Pak $\mathbf{A}$ je typu (11.1).

Nechť $\boldsymbol{u} \in V$ má souřadnice $\boldsymbol{c} \in \mathbf{R}^n$ vzhledem k (O, B). Pak má homogenní souřadnice $(\boldsymbol{c}, 0)$ a platí:

$$\mathbf{A} \cdot \begin{pmatrix} \boldsymbol{c}^T \\ 0 \end{pmatrix} = \begin{pmatrix} \mathbf{A}' & \boldsymbol{t} \\ \boldsymbol{o} & 1 \end{pmatrix} \cdot \begin{pmatrix} \boldsymbol{c}^T \\ 0 \end{pmatrix} = \begin{pmatrix} \mathbf{A}' \cdot \boldsymbol{c}^T \\ 0 \end{pmatrix}$$

takže maticové násobení $\mathbf{A}\cdot\boldsymbol{x}$ transformuje také homogenní souřadnice vektorů na homogenní souřadnice vektorů. K této transformaci homogenních souřadnic vektorů existuje zpětně transformace vektorů samotných $\mathcal{A}' : V \to V$ taková že homogenní souřadnice obrazu $\mathcal{A}'(\boldsymbol{u})$ jsou rovny sloupcovému vektoru

$$\mathbf{A}\cdot\begin{pmatrix}\boldsymbol{c}^T\\0\end{pmatrix}.$$

Tato transformace $\mathcal{A}' : V \to V$ je zjevně lineární a má matici $\mathbf{A}'$ vzhledem k bázi (B).

Nyní stačí dokázat, že $\mathcal{A}(P+\boldsymbol{u}) = \mathcal{A}(P) + \mathcal{A}'(\boldsymbol{u})$ pro všechny body $P \in \mathbf{X}$ a všechny vektory $\boldsymbol{u} \in V$. Tato rovnost platí, protože

$$\mathbf{A}\cdot\left(\begin{pmatrix}\boldsymbol{p}^T\\1\end{pmatrix}+\begin{pmatrix}\boldsymbol{c}^T\\0\end{pmatrix}\right)=\mathbf{A}\cdot\begin{pmatrix}\boldsymbol{p}^T\\1\end{pmatrix}+\mathbf{A}\cdot\begin{pmatrix}\boldsymbol{c}^T\\0\end{pmatrix}$$

11.24. Věta.* Nechť $(\mathbf{X}, V)$ je afinní prostor dimenze n se souřadnicovým systémem (O, B). Pak každé afinní zobrazení $\mathcal{A}$ má matici $\mathbf{A}$ v homogenních souřadnicích vzhledem k (O, B).

Důkaz. Protože $\mathcal{A}$ je afinní, existuje lineární transformace $\mathcal{A}' : V \to V$ tak, že $\mathcal{A}(P+\boldsymbol{u}) = \mathcal{A}(P) + \mathcal{A}'(\boldsymbol{u})$ pro všechny body $P \in \mathbf{X}$ a všechny vektory $\boldsymbol{u} \in V$. Do matice $\mathbf{A}$ zapíšeme nejprve homogenní souřadnice obrazů bázových vektorů $\mathcal{A}'(\boldsymbol{b}_i)$ a do posledního sloupce zapíšeme obraz $\mathcal{A}(O)$. Takto sestavená matice je zjevně typu (11.1). Označme $\mathcal{B} : \mathbf{X} \to \mathbf{X}$ transformaci, která má matici $\mathbf{A}$ v homogenních souřadnicích. Podle věty ?? je $\mathcal{B}$ afinní transformace. Když

ukážeme, že $\mathcal{B}(O) = \mathcal{A}(O)$ a dále $\mathcal{B}(O + \boldsymbol{b}_i) = \mathcal{A}(O + \boldsymbol{b}_i)$ pro všechny bázové vektory $\boldsymbol{b}_i$, budeme podle věty ?? vědět, že $\mathcal{A} = \mathcal{B}$, tedy $\mathcal{A}$ má matici $\mathbf{A}$.

Homogenní souřadnice počátku O jsou všude nulové s výjimkou poslední složky, kde je jednička. Vektor těchto souřadnic označme $\boldsymbol{e}_{n+1} \in \mathbf{R}^{n+1}$. Homogenní souřadnice $\mathcal{B}(O)$ se počítají podle vzorce $\mathbf{A} \cdot \boldsymbol{e}_{n+1}^T$ a tento součin je roven poslednímu sloupci matice $\mathbf{A}$. Ten podle pravidla sestavení matice $\mathcal{A}$ obsahuje homogenní souřadnice obrazu $\mathcal{A}(O)$. Takže $\mathcal{B}(O) = \mathcal{A}(O)$. Homogenní souřadnice bázového vektoru $\boldsymbol{b}_i$ jsou všude nulové s výjimkou i-té složky. Vektor těchto souřadnic označme $\boldsymbol{e}_i \in \mathbf{R}^{n+1}$. Homogenní souřadnice $\mathcal{B}(O+\boldsymbol{b}_i)$ počítáme podle vzorce $\mathbf{A} \cdot (\boldsymbol{e}_{n+1}^T + \boldsymbol{e}_i^T)$. Tento součin je roven součtu i-tého sloupce matice $\mathbf{A}$ s posledním, tedy obsahuje (podle pravidla sestavení matice) homogenní souřadnice obrazu $\mathcal{A}(O) + \mathcal{A}'(\boldsymbol{b}_i) = \mathcal{A}(O + \boldsymbol{b}_i)$. Z toho plyne $\mathcal{B}(O + \boldsymbol{b}_i) = \mathcal{A}(O + \boldsymbol{b}_i)$.

11.25. Věta. *Nechť má afinní prostor $(\mathbf{X}, V)$ dimenzi n. Afinní transformace $\mathcal{A} \colon \mathbf{X} \to \mathbf{X}$ je prostá právě tehdy, když je na.*

Důkaz. Afinní transformace $\mathcal{A} \colon \mathbf{X} \to \mathbf{X}$ je prostá právě tehdy, když její přidružená lineární transformace $\mathcal{A}' : V \to V$ je prostá, právě tehdy, když $\operatorname{def} \mathcal{A}' = 0$ právě tehdy, když $\operatorname{hod} \mathcal{A}' = n$ (viz větu ??) právě tehdy, když $\mathcal{A}'$ je na V právě tehdy, když $\mathcal{A}$ je na $\mathbf{X}$.

11.26. Věta.* *Složení dvou afinních transformací je afinní transformace.*

Důkaz. Ve větě ?? jsme ukázali, že složením dvou transformací, které mají svou matici v homogenních souřadnicích, je transfrormace, která má matici v homogenních souřadnicích. Dále ve větách ?? a ?? jsme ukázali, že tranfsormace má matici v homogenních souřadnicích právě tehdy, když je afinní.

11.27. Věta. Inverzní transformace k prosté afinní transformaci je afinní.

Důkaz. Má-li původní transformace matici $\mathbf{A}$ v homogenních souřadnicích, pak inverzní transformace má matici $\mathbf{A}^{-1}$ v homogenních souřadnicích.

11.28. Věta. Prostá afinní transformace transformuje rovnoběžné přímky na rovnoběžné přímky.

Důkaz. Přímka v afinním prostoru $(\mathbf{X}, V)$ je množina $p = \{P + t\boldsymbol{u};\, t \in \mathbf{R}\}$, kde $P \in \mathbf{X}$ je nějaký bod a $\boldsymbol{u} \in V$ je nenulový vektor. Vektoru $\boldsymbol{u}$ v tomto kontextu říkáme *směrový vektor přímky*. Dvě přímy jsou rovnoběžné nebo totožné, pokud jejich směrové vektory jsou lineárně závislé (tedy jeden je nenulovým násobkem druhého).

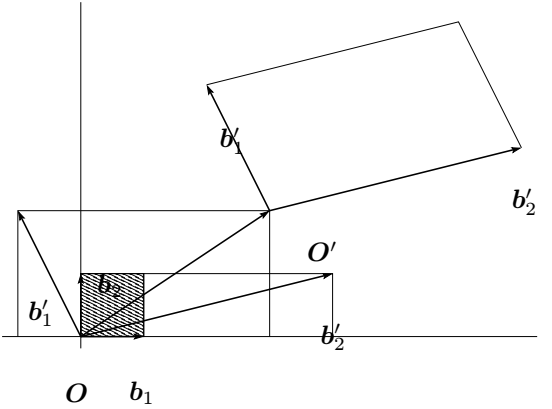
Nechť $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$ je prostá afinní transformace a označme $p = \{P + t\boldsymbol{u};\, t \in \mathbf{R}\}$ a $q = \{Q + t\boldsymbol{v};\, t \in \mathbf{R}\}$ dvě různé rovnoběžné přímky. Takže $\boldsymbol{u} = \alpha\boldsymbol{v}$. Pak

$$\mathcal{A}(p) = \{\mathcal{A}(P + t\boldsymbol{u});\, t \in \mathbf{R}\} = \{\mathcal{A}(P) + \mathcal{A}'(t\boldsymbol{u});\, t \in \mathbf{R}\} = \{\mathcal{A}(P) + t\mathcal{A}'(\boldsymbol{u});\, t \in \mathbf{R}\} = p'$$
$$\mathcal{A}(q) = \{\mathcal{A}(Q + t\boldsymbol{v});\, t \in \mathbf{R}\} = \{\mathcal{A}(Q) + \mathcal{A}'(t\boldsymbol{v});\, t \in \mathbf{R}\} = \{\mathcal{A}(Q) + t\mathcal{A}'(\boldsymbol{v});\, t \in \mathbf{R}\} = q'$$

Je zřejmé, že p' a q' jsou přímky. Protože $\mathcal{A}$ je prosté, je prosté také $\mathcal{A}'$, takže vektory $\mathcal{A}'(\boldsymbol{u})$ a $\mathcal{A}'(\boldsymbol{u})$ jsou nenulové. Přímky p' a q' jsou rovnoběžné protože $\mathcal{A}'(\boldsymbol{u}) = \mathcal{A}'(\alpha\boldsymbol{v}) = \alpha\mathcal{A}'(\boldsymbol{v})$. Navíc nejsou totožné, protože $\mathcal{A}$ je prosté.

11.29. Poznámka. Předpokládejme nyní, že afinní zobrazení není prosté. V tomto případě se přímky mohou zobrazit do bodu nebo dvě rovnoběžné přímky se zobrazí do jedné přímky. Projděte si důkaz předchozí věty znova a rozmyslete si, že afinní zobrazení, které nemusí být prosté, nikdy nezobrazí rovnoběžky na různoběžky.

11.30. Příklad. V afinním prostoru dimenze 2 najdeme matici $\mathbf{A}$ v homogenních souřadnicích takové afinní transformace, která zobrazí $\boldsymbol{b}_1$ na $\boldsymbol{b}'_1$, dále $\boldsymbol{b}_2$ zobrazí na $\boldsymbol{b}'_2$ a konečně O zobrazí na O' podle obrázku. Tato transformace například vezme obrázek z vyšrafovaného čtverce a protáhne jej, zkosí jej, zrcadlí jej (osová souměrnost), otočí jej a posune jej a tím vytvoří obraz původního obrázku ve vyznačeném rovnoběžníku.



Uvědomíme si, že pokud je dána báze $(\boldsymbol{b}_1, \boldsymbol{b}_2)$ a pokud jsou dány vektory $\boldsymbol{b}'_1$ a $\boldsymbol{b}'_2$,

pro které má být $\boldsymbol{b}'_i = \mathcal{A}'(\boldsymbol{b}_i)$ pro $i \in \{1,2\}$,
pak lineární transformace $\mathcal{A}' : V \to V$ s uvedenou vlastností podle věty ?? existuje a je jediná. Když k tomu přidáme požadavek na posunutí bodu O do O', je tím také určena transformace $\mathcal{A} : \mathbf{X} \to \mathbf{X}$. Matice této transformace má podle důkazu věty ?? homogenní souřadnice vektorů $\boldsymbol{b}'_i$ a bodu O' v odpovídajících sloupcích. Aby se nám na obrázku souřadnice vektorů $\boldsymbol{b}'_i$ vzhledem k bázi (B) dobře hledaly, překreslili jsme jejich orientované úsečky také tak, aby začínaly v bodě O. Vidíme, že

$$\begin{aligned}
\boldsymbol{b}'_1 &= -1 \cdot \boldsymbol{b}_1 + 2 \cdot \boldsymbol{b}_2, && \text{takže vektor } \boldsymbol{b}'_1 \text{ má souřadnice } (-1,2) \text{ vzhledem k } (B),\\
\boldsymbol{b}'_2 &= 4 \cdot \boldsymbol{b}_1 + 1 \cdot \boldsymbol{b}_2, && \text{takže vektor } \boldsymbol{b}'_2 \text{ má souřadnice } (4,1) \text{ vzhledem k } (B),\\
O' - O &= 3 \cdot \boldsymbol{b}_1 + 2 \cdot \boldsymbol{b}_2, && \text{takže bod } O' \text{ má souřadnice } (3,2) \text{ vzhledem k } (O,B).
\end{aligned}$$

Hledanou matici $\mathbf{A}$ nyní vyplníme po sloupcích homogenními souřadnicemi vektorů $\boldsymbol{b}'_1$, $\boldsymbol{b}'_2$ a bodu O':

$$\mathbf{A} = \begin{pmatrix} -1 & 4 & 3 \\ 2 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

11.31. Poznámka. Dá se ukázat, že každá afinní transformace afinního prostoru dimenze 2 je výsledkem skládání elementárních operací změny měřítka, otočení a posunutí uvedených v příkladu ??. Důkaz tohoto tvrzení ponecháme až do kapitoly ?? v příkladu ??.

11.32. Poznámka. V počítačové grafice se řeší otázka zobrazení 3D modelu na 2D stínítko monitoru. Můžeme to udělat odstraněním například souřadnice z ze tří původních souřadnic 3D modelu, tedy $(x, y, z) \to (x, y)$. Toto zobrazení nazýváme ortografickou projekcí. Přirozenější ale je představit si oko pozorovatele (nebo kameru) jako centrum, do kterého se sbíhají všechny paprsky odrážející se od pozorovaných objektů. Před pozorovatele postavíme stínítko monitoru – průhlednou rovinu. Každý pozorvaný bod má svůj paprsek směřující do oka a průsečík tohoto paprsku s rovinou stínítka je obraz pozorovaného bodu při perspektivní projekci. Situace je znázorněná na obrázku. Zde je oko pozorovatele umístěné do počátku souřadnic afinního prostoru a rovina stínítka je kolmá na osu z a je umístěna ve vzdálenosti 1 od pozorovatele. Pozorovatel se dívá „nahoru“. Je docela pohodlné ležet na gauči a zírat vzhůru. Za této situace se bod 3D scény se souřadnicemi (x, y, z) zobrazí na stínítko do místa se souřadnicemi $(x/z, y/z, 1)$ a po zanedbání souřadnice z máme výsledné 2D souřadnice $(x/z, y/z)$. Tuto perpektivní projekci tedy můžeme popsat jako $(x, y, z) \to (x/z, y/z)$. Zjevně body se souřadnicemi $(x, y, 0)$ původní 3D scény nejsou vidět a do 2D scény se nezobrazují. Pravda, nejsou vidět ani body za zády pozorovatele, tj. (x, y, z) pro $z < 0$. Pokud bychom je před projekcí neodstranili, pak by se nám při použití vzorce $(x, y, z) \to (x/z, y/z)$ také promítly do stínítka.

Perspektivní projekce není afinní zobrazení. Zobrazuje sice přímky (neprocházející okem) na přímky, ale rovnoběžné přímky se mohou sbíhat ve společném bodě, což není podle ?? vlastnost afinního zobrazení. V předchozím textu jsme ukázali, že matice všech afinních zobrazení v homogenních souřadnicích mají v posledním řádku $(0, \ldots, 0, 1)$. Dovolíme-li maticím ne-

mít tuto vlastnost, můžeme pomocí maticového násobení postihnout i perspektivní projekci. Potřebujeme k tomu účelu ovšem rozšířit pojem homogenní souřadnice bodu. V poslední souřadnici od této chvíle připustíme jakékoli nenulové číslo, ne nutně jedničku:

11.33. Definice.* Nechť $(\mathbf{X}, V)$ je afinní prostor a (O, B) jeho souřadnicový systém. Nechť bod $P \in \mathbf{X}$ má vzhledem k (O, B) souřadnice $(x_1, x_2, \ldots, x_n)$. Pak jakoukoli uspořádanou $(n+1)$-tici $(tx_1, tx_2, \ldots, tx_n, t)$ pro $t \neq 0$ nazýváme *homogenní souřadnice bodu* P.

11.34. Poznámka. Homogenní souřadnice bodu nejsou určeny touto definicí jednoznačně. Můžeme použít následující geometrickou představu: všechny homogenní souřadnice stejného bodu P z afinního prostoru $(\mathbf{X}, V)$ dimenze n vyplní (až na počátek) přímku v prostoru $\mathbf{R}^{n+1}$ homogenních souřadnic. Tato přímka vždy prochází počátkem prostoru $\mathbf{R}^{n+1}$. V prostoru homogenních souřadnic $\mathbf{R}^{n+1}$ si vytvořme zobecněnou rovinu $\varrho = \{(x_1, x_2, \ldots, x_n, 1),\, x_i \in \mathbf{R}\}$. Bod P je v prostoru homogenních souřadnic reprezentován přímkou, která protíná rovinu ϱ v bodě P (po zanedbání poslední souřadnice). Všechny objekty v $\mathbf{X}$ mají v prostoru homogenních souřadnic o jednu dimenzi více, než v $\mathbf{X}$ samotném. Například přímka v $\mathbf{X}$ je rovinou v $\mathbf{R}^{n+1}$ procházející počátkem. Přitom průsečík této roviny se zobecněnou rovinou ϱ dává původní přímku.

11.35. Poznámka. Pro popis perspektivní projekce 3D scény na 2D stínítko si vystačíme s afinním prostorem dimenze 3 a se čtyřmi homogenními souřadnicemi na vstupu a s afinním

prostorem dimenze 2 a třemi homogenními souřadnicemi na výstupu. Popíšeme perspektivní projekci, která je ve skutečných souřadnicích popsána vzorcem $(x, y, z) \to (x/z, y/z)$ a byla zmíněna v poznámce ??. Nechť homogenní souřadnice vzoru v této projekci jsou $(x, y, z, 1)$. Homogenní souřadnice obrazu jsou třeba $(x/z, y/z, 1)$, ale stejný bod má též (v souladu s definicí ?? a při volbě $t = z$) homogenní souřadnice (x, y, z). Matice perspektivní projekce v homogenních souřadnicích tedy vypadá následovně:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad \text{protože} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \\ 1 \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

Povšimneme si, že na vstupu máme bod z 3D popsaný čtyřmi homogenními souřadnicemi a na výstupu bod z 2D popsaný třemi homogenními souřadicemi. Bod na výstupu nemá poslední homogenní souřadnici vždy rovnu jedné. Chceme-li zjistit skutečné souřadnice tohoto bodu, musíme najít jiné homogenní souřadnice stejného bodu, které mají v poslední složce jedničku. Tedy: $(x/z, y/z, 1)$. Skutečné 2D souřadnice tedy podle očekávání jsou $(x/z, y/z)$.

11.36. Shrnutí. Afinní prostor sestává z množiny bodů **X** a z lineárního prostoru V /??/. Je definována operace „bod plus vektor je bod“, která splňuje axiomy (1) až (3) /??/.

Souřadnice bodu P jsou souřadnice jeho radiusvektoru $P - O$. Souřadnice bodů i vektorů zachovávají potřebné operace /??/.

Homogenní souřadnice bodu jsou souřadnice bodu následované jedničkou a homogenní souřadnice vektoru jsou souřadnice vektoru následované nulou /??/.

Transformace $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$ jsou afinní, právě když mají matici v homogenních souřadnicích /??, ??, ??, ??/. Skládání afinních transformací má v homogenních souřadnicích matici rovnou součinu matic jednotlivých transformací.

Matice v homogenních souřadnicích má vždy v posledním řádku $(0, \ldots, 0, 1)$.

Uvedli jsme si matice elementárních transformací: změna měřítka, rotace a posunutí /??/. Skládáním elementárních transformací lze vytvořit libovolnou afinní transformaci.

Nechť $(\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n, O)$ je souřadnicový systém prostoru $(\mathbf{X}, V)$ Afinní transformace $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$ je jednoznačně určena svými obrazy bodu O a bodů $O + \boldsymbol{b}_i$ /??/. Matice této transformace v homogeních souřadnicích má ve sloupcích homogenní souřadnice obrazů $\boldsymbol{b}_i$ následované sloupcem s homogenními souřadnicemi obrazu bodu O.

12. Vlastní číslo, vlastní vektor

12.1. Příklad. Předpokládejme, že je dána lineární transformace $\mathcal{A}\colon \mathbf{R}^2 \to \mathbf{R}^2$, která má svou matici $\mathbf{A} \in \mathbf{R}^{2,2}$. Je-li $\boldsymbol{u} \in \mathbf{R}^2$ nenulový vektor, pak množina $p = \{t\boldsymbol{u};\, t \in \mathbf{R}\}$ je (z geometrického pohledu) přímka, procházející počátkem. Nenulovému vektoru $\boldsymbol{u}$ říkáme *směrový vektor přímky*. Transformace $\mathcal{A}$ zobrazuje přímky procházející počátkem na přímky procházející počátkem. Pokusíme se najít přímku procházející pořátkem, která se tranformací $\mathcal{A}$ zobrazí sama na sebe.

Hledanou přímku označíme $p = \{t\boldsymbol{u};\, t \in \mathbf{R}\}$. Musí platit $p = \mathcal{A}(p) = \{t\mathcal{A}(\boldsymbol{u});\, t \in \mathbf{R}\}$, takže směrový vektor přímky p a směrový vektor přímky $\mathcal{A}(p)$ musejí být lineárně závislé, tedy $\mathcal{A}(\boldsymbol{u}) = \lambda\boldsymbol{u}$.

Je-li dána matice $\mathbf{A}$ zobrazení $\mathcal{A}$, pak se předchozí úloha dá formulovat takto: najít nenulový vektor $\boldsymbol{u} \in \mathbf{R}^2$ a číslo $\lambda \in \mathbf{R}$ tak, aby $\mathbf{A} \cdot \boldsymbol{u} = \lambda\boldsymbol{u}$. Rovnost se dá přepsat takto: $\mathbf{A} \cdot \boldsymbol{u} = \lambda\mathbf{E} \cdot \boldsymbol{u}$, neboli $(\mathbf{A} - \lambda\mathbf{E}) \cdot \boldsymbol{u} = \boldsymbol{o}$. Aby bylo možné najít nenulové řešení $\boldsymbol{u}$ této homogenní soustavy (s parametrem $\lambda \in \mathbf{R}$), musí její matice $\mathbf{A} - \lambda\mathbf{E}$ být singulární, neboli musí $\det(\mathbf{A} - \lambda\mathbf{E}) = 0$. Je-li dána matice $\mathbf{A} \in \mathbf{R}^2$, pak rovnice $\det(\mathbf{A} - \lambda\mathbf{E}) = 0$ je kvadratická rovnice v proměnné λ. Tato rovnice může, ale nemusí mít reálné kořeny. Pokud má reálné kořeny λ_1 a λ_2, pak lze najít nenulová řešení homogenních soustav $(\mathbf{A} - \lambda_1\mathbf{E}) \cdot \boldsymbol{u} = \boldsymbol{o}$ a $(\mathbf{A} - \lambda_2\mathbf{E}) \cdot \boldsymbol{u} = \boldsymbol{o}$. Označíme-li tato řešení $\boldsymbol{u}_1$ a $\boldsymbol{u}_2$, pak jsme našli dvě přímky $p_1 = \{t\boldsymbol{u}_1\}$

a $p_2 = \{t\boldsymbol{u}_2\}$, které se zobrazí na sebe. Uvedený postup ukážeme v následujících příkladech znovu a konkrétněji.

12.2. Příklad. Nechť lineární transformace $\mathcal{A}\colon \mathbf{R}^2 \to \mathbf{R}^2$ má matici

$$\mathbf{A} = \begin{pmatrix} 5 & 2 \\ -3 & 0 \end{pmatrix}$$

Najdeme přímky, které tato transformace ponechá beze změny.

Nechť $p = \{t(x_1, x_2);\ t \in \mathbf{R}\}$ je hledaná přímka. Musí platit $\mathcal{A}(x_1, x_2) = \lambda(x_1, x_2)$, neboli:

$$\begin{pmatrix} 5 & 2 \\ -3 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \lambda \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \quad \text{tj.} \quad \begin{pmatrix} 5-\lambda & 2 \\ -3 & -\lambda \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Protože hledaný vektor (x_1, x_2) musí být nenulový, musí mít uvedená homogenní soustava singulární matici. To znamená, že:

$$\det \begin{pmatrix} 5-\lambda & 2 \\ -3 & -\lambda \end{pmatrix} = 0, \quad \text{tj.} \quad \lambda^2 - 5\lambda + 6 = 0, \quad \text{tj.} \quad \lambda = 2 \quad \text{nebo} \quad \lambda = 3.$$

Kořeny $\lambda = 2$ a $\lambda = 3$ postupně dosadíme do původní homogenní soustavy:

$$\lambda = 2\colon \quad \begin{pmatrix} 5-2 & 2 \\ -3 & -2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \qquad \lambda = 3\colon \quad \begin{pmatrix} 5-3 & 2 \\ -3 & -3 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Nenulové řešení první soustavy je například $(-2, 3)$ a nenulové řešení druhé soustavy je $(-1, 1)$. Takže přímky $p_1 = \{t(-2, 3);\, t \in \mathbf{R}\}$ a $p_2 = \{t(-1, 1);\, t \in \mathbf{R}\}$ jsou hledané přímky, které se zobrazí na sebe.

12.3. Příklad. Nechť lineární transformace $\mathcal{A}\colon \mathbf{R}^2 \to \mathbf{R}^2$ má matici

$$\mathbf{A} = \begin{pmatrix} 1 & 2 \\ -2 & 3 \end{pmatrix}$$

Najdeme přímky, které tato transformace ponechá beze změny.

Postup nebudeme opakovat podrobně znovu. V jedné fázi výpočtu dostáváme determinant:

$$\det \begin{pmatrix} 1-\lambda & 2 \\ -2 & 3-\lambda \end{pmatrix} = 0, \quad \text{tj.} \quad \lambda^2 - 4\lambda + 7 = 0, \quad \text{tato rovnice nemá v } \mathbf{R} \text{ řešení.}$$

V tomto případě neexistuje žádná přímka procházející počátkem, kterou by daná lineární transformace ponechala beze změny.

12.4. Poznámka. Číslům λ v předchozích příkladech se říká *vlastní čísla matice* $\mathbf{A}$, resp. *vlastní čísla transformace* $\mathcal{A}$. Směrovým vektorům přímek, které transformace ponechává beze změny, říkáme *vlastní vektory*. Přesnější definici těchto pojmů zavedeme za chvíli.

12.5. Poznámka. Z uvedených příkladů plyne, že vlastní čísla matice $\mathbf{A}$ lze počítat jako kořeny polynomu $\det(\mathbf{A} - \lambda\mathbf{E})$. Tyto kořeny ovšem nemusejí být vždy reálné. Abychom měli zaručenu vždy existenci vlastního čísla, budeme muset připustit i komplexní vlastní čísla a komplexní vlastní vektory. V této kapitole tedy bude užitečné pracovat s lineárními prostory nad komplexními čísly (viz poznámku ??) a s komplexními maticemi. Pak budeme mít zaručeno, že každá lineární transformace (resp. její matice) má vždy vlastní čísla a vlastní vektory. Bohužel, přechodem ke komplexním číslům musíme poněkud více přimhouřit obě oči, když chceme vlastní vektory interpretovat geometricky jako směrové vektory přímek, které transformace ponechává beze změny. Geometrický prostor, na který jsme zvyklí, je totiž izomorfní s $\mathbf{R}^3$, nikoli s $\mathbf{C}^3$.

V modelových příkladech se pokusíme komplexním číslům vyhnout.

12.6. Definice.* Nechť L je lineární prostor konečné dimenze nad $\mathbf{C}$ a nechť $\mathcal{A}\colon L \to L$ je lineární transformace. Číslo $\lambda \in \mathbf{C}$ se nazývá *vlastním číslem transformace $\mathcal{A}$*, pokud existuje vektor $\boldsymbol{x} \in L$, $\boldsymbol{x} \neq \boldsymbol{o}$ takový, že $\mathcal{A}(\boldsymbol{x}) = \lambda\,\boldsymbol{x}$. Vektor $\boldsymbol{x}$, který splňuje uvedenou rovnost, se nazývá *vlastní vektor transformace $\mathcal{A}$ příslušný vlastnímu číslu λ*.

12.7. Poznámka. Pokud existuje vlastní číslo transformace $\mathcal{A}$, pak mu přísluší více vlastních vektorů. Přidáme-li k těmto vektorům vektor nulový, dostáváme lineární podprostor prostoru L. Skutečně, pokud $\boldsymbol{x}$, $\boldsymbol{y}$ splňují $\mathcal{A}(\boldsymbol{x}) = \lambda\,\boldsymbol{x}$, $\mathcal{A}(\boldsymbol{y}) = \lambda\,\boldsymbol{y}$, pak

$$\mathcal{A}(\boldsymbol{x}+\boldsymbol{y}) = \mathcal{A}(\boldsymbol{x}) + \mathcal{A}(\boldsymbol{y}) = \lambda\,\boldsymbol{x} + \lambda\,\boldsymbol{y} = \lambda\,(\boldsymbol{x}+\boldsymbol{y}), \qquad \mathcal{A}(\alpha\,\boldsymbol{x}) = \alpha\,\mathcal{A}(\boldsymbol{x}) = \alpha\lambda\,\boldsymbol{x} = \lambda\,(\alpha\,\boldsymbol{x}).$$

12.8. Poznámka. Pojem vlastní číslo definujeme nejenom pro lineární transformace, ale rovněž pro čtvercové matice. Záhy zjistíme, že mezi vlastním číslem transformace a její matice je úzká souvislost.

12.9. Definice.* Nechť $\mathbf{A}$ je čtvercová matice typu (n, n) reálných nebo komplexních čísel. Číslo $\lambda \in \mathbf{C}$ se nazývá *vlastním číslem matice* $\mathbf{A}$, pokud existuje vektor $\boldsymbol{x} \in \mathbf{C}^{n,1}$, $\boldsymbol{x} \neq \boldsymbol{o}$, takový, že $\mathbf{A} \cdot \boldsymbol{x} = \lambda \boldsymbol{x}$. Vektor $\boldsymbol{x}$, který splňuje uvedenou rovnost, se nazývá *vlastní vektor matice* $\mathbf{A}$ *příslušný vlastnímu číslu* λ.

12.10. Věta. Nechť $\mathcal{A}\colon L \to L$ je lineární transformace a $\mathbf{A}$ je jeho matice vzhledem k nějaké bázi (B). Pak λ je vlastním číslem transformace $\mathcal{A}$ právě tehdy, když je vlastním číslem matice $\mathbf{A}$. Navíc $\boldsymbol{x}$ je vlastní vektor transformace $\mathcal{A}$ příslušný λ právě tehdy, když souřadnice vektoru $\boldsymbol{x}$ vzhledem k bázi (B) tvoří vlastní vektor matice $\mathbf{A}$ příslušný λ.

Důkaz. Označme $\boldsymbol{u} \in \mathbf{C}^n$ souřadnice vektoru $\boldsymbol{x}$ v bázi (B). Podle věty ?? sloupec $\mathbf{A} \cdot \boldsymbol{u}$ obsahuje souřadnice obrazu $\mathcal{A}(\boldsymbol{x})$ vzhledem k bázi (B). Takže $\mathcal{A}(\boldsymbol{x}) = \lambda \boldsymbol{x}$ právě tehdy, když $\mathbf{A} \cdot \boldsymbol{u} = \lambda \boldsymbol{u}$.

12.11. Poznámka. Množina všech vlastních čísel lineární transformace nebo matice se nazývá *spektrum*. Vlastním číslům/vektorům někteří čeští autoři říkají *charakteristická čísla/vekto* (anglicky eigenvalue, eigenvector, což je odvozeno z němčiny).

12.12. Poznámka. Přikročíme nyní k výpočtu vlastních čísel, je-li dána čtvercová matice $\mathbf{A}$. Vyjdeme z rovnosti $\mathbf{A} \cdot \boldsymbol{x} = \lambda \boldsymbol{x} = \lambda \mathbf{E} \cdot \boldsymbol{x}$. Z obou stran této rovnice odečteme $\lambda \mathbf{E} \cdot \boldsymbol{x}$. Dostáváme vztah $\mathbf{A} \cdot \boldsymbol{x} - \lambda \mathbf{E} \cdot \boldsymbol{x} = (\mathbf{A} - \lambda \mathbf{E}) \cdot \boldsymbol{x} = \boldsymbol{o}$. Z definice vlastního čísla víme, že příslušný vlastní vektor $\boldsymbol{x}$ musí být nenulový. Je tedy zřejmé, že λ bude vlastním číslem matice $\mathbf{A}$ právě tehdy, když homogenní soustava s maticí $\mathbf{A} - \lambda \mathbf{E}$ bude mít nenulové řešení. Tímto řešením pak bude vlastní vektor příslušný vlastnímu číslu λ. Aby tato soustava měla nenulové řešení, musí její matice být singulární, tj. musí $\det(\mathbf{A} - \lambda \mathbf{E}) = 0$. Tím máme odvozen vzorec na výpočet vlastních čísel. Uvědomíme si ještě, že $\det(\mathbf{A} - \lambda \mathbf{E})$ je polynom v proměnné λ. Tento polynom se nazývá *charakteristický polynom* matice $\mathbf{A}$. Jeho stupeň je stejný, jako počet řádků matice $\mathbf{A}$. Označme toto číslo n. Abychom tedy našli všechna vlastní čísla dané matice, stačí najít všechny kořeny charakteristického polynomu této matice. Podle základní věty algebry těchto kořenů (včetně jejich násobnosti) je n. Každá matice má tedy n vlastních čísel (obecně ne vzájmeně různých). Každá lineární transformace $\mathcal{A} \colon L \to L$ má tolik vlastních čísel, kolik je dimeze L.

12.13. Definice. Nechť $\mathbf{A}$ je čtvercová matice. Polynom $\det(\mathbf{A} - \lambda \mathbf{E})$ nazýváme *charakteristický polynom matice* $\mathbf{A}$ a rovnost $\det(\mathbf{A} - \lambda \mathbf{E}) = 0$ charakteristickou rovnicí. Je-li λ k-násobným kořenem charakteristické rovnice, říkáme, že λ je *k-násobným vlastním číslem*.

12.14. Příklad. Uvedeme ještě celý postup odvození výpočtu vlastních čísel matice (viz předchozí poznámku) znovu na konkrétním numerickém příkladě, protože odvození může pro

někoho být na konkrétním příkladě názornější. Budeme hledat vlastní čísla a vlastní vektory matice

$$\mathbf{A} = \begin{pmatrix} 5 & -2 & 2 \\ -1 & 4 & -1 \\ -4 & 4 & -1 \end{pmatrix}.$$

Podle definice ?? hledáme takové číslo λ a vektor $\boldsymbol{x} = (x_1, x_2, x_3)$, aby byla splněna maticová rovnost

$$\begin{pmatrix} 5 & -2 & 2 \\ -1 & 4 & -1 \\ -4 & 4 & -1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \lambda \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix},$$

a přitom vektor $\boldsymbol{x}$ byl nenulový. Rozepíšeme tuto rovnost do složek:

$$\begin{array}{rcl} 5x_1 - 2x_2 + 2x_3 = \lambda x_1 \\ -x_1 + 4x_2 - x_3 = \lambda x_2 \\ -4x_1 + 4x_2 - x_3 = \lambda x_3 \end{array} \qquad \text{tj.} \qquad \begin{array}{rcl} (5-\lambda)x_1 - 2x_2 + 2x_3 = 0 \\ -x_1 + (4-\lambda)x_2 - x_3 = 0 \\ -4x_1 + 4x_2 + (-1-\lambda)x_3 = 0 \end{array}$$

Potřebujeme, aby uvedená homogenní soustava se čtvercovou maticí měla nenulové řešení. Matice soustavy tedy musí být singulární, tj. musí mít nulový determinant:

$$\det \begin{pmatrix} 5-\lambda & -2 & 2 \\ -1 & 4-\lambda & -1 \\ -4 & 4 & -1-\lambda \end{pmatrix} = 0.$$

Hledáme tedy λ takové, aby $\det(\mathbf{A}-\lambda\mathbf{E})=0$. Příště už toto odvození nebudeme opakovat, ale začneme rovnou od rovnice $\det(\mathbf{A}-\lambda\mathbf{E})=0$.

$$\det(\mathbf{A}-\lambda\mathbf{E}) = (5-\lambda)(4-\lambda)(-1-\lambda)-16-\big(-8(4-\lambda)-4(5-\lambda)+2(-1-\lambda)\big) = -(\lambda-3)^2(\lambda-2),$$

takže vlastní čísla jsou $\lambda=3$ a $\lambda=2$. Najdeme ještě vlastní vektory. Nejprve najdeme vlastní vektory příslušné vlastnímu číslu 3:

$$\begin{pmatrix} 5-3 & -2 & 2 \\ -1 & 4-3 & -1 \\ -4 & 4 & -1-3 \end{pmatrix} = \begin{pmatrix} 2 & -2 & 2 \\ -1 & 1 & -1 \\ -4 & 4 & -4 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & 1 \end{pmatrix}.$$

Báze řešení homogenní soustavy s maticí $(1\ -1\ \ 1)$ je například $\{(1,1,0),(-1,0,1)\}$. Toto jsou dva lineárně nezávislé vlastní vektory, které přísluší vlastnímu číslu 3. Všechny vlastní vektory příslušející vlastnímu číslu 3 tvoří lineární obal této báze, ovšem bez nulového vektoru. Nyní najdeme vlastní vektory, které přísluší vlastnímu číslu 2:

$$\begin{pmatrix} 5-2 & -2 & 2 \\ -1 & 4-2 & -1 \\ -4 & 4 & -1-2 \end{pmatrix} = \begin{pmatrix} 3 & -2 & 2 \\ -1 & 2 & -1 \\ -4 & 4 & -3 \end{pmatrix} \sim \begin{pmatrix} -1 & 2 & -1 \\ 0 & 4 & -1 \\ 0 & -4 & 1 \end{pmatrix} \sim \begin{pmatrix} -1 & 2 & -1 \\ 0 & 4 & -1 \end{pmatrix}.$$

Dimenze prostoru řešení homogenní soustavy s touto maticí je 1, tj. stačí najít jeden vektor řešení: $(-2,1,4)$ a ostatní vektory řešení jsou jeho násobky. Tato řešení (bez nulového) jsou též všechny vlastní vektory matice $\mathbf{A}$, které přísluší vlastnímu číslu 2.

Celkem tedy má matice $\mathbf{A}$ tři lineárně nezávislé vlastní vektory: $(1,1,0), (-1,0,1), (-2,1,4)$. První dva příslušejí vlastnímu číslu 3 a poslední přísluší vlastnímu číslu 2.

12.15. Příklad. Následující příklad ukazuje, že nemusí existovat tolik lineárně nezávislých vlastních vektorů, kolik řádků má matice. Budeme hledat vlastní čísla a vlastní vektory matice:

$$\mathbf{A} = \begin{pmatrix} 2 & 4 & -3 \\ -1 & 10 & -6 \\ -1 & 8 & -4 \end{pmatrix}.$$

Vypočteme determinant matice $\mathbf{A} - \lambda\mathbf{E}$:

$$\det \begin{pmatrix} 2-\lambda & 4 & -3 \\ -1 & 10-\lambda & -6 \\ -1 & 8 & -4-\lambda \end{pmatrix} = -(\lambda-3)^2(\lambda-2).$$

Vidíme, že matice má stejná vlastní čísla, jako matice z předchozího příkladu. Nyní vypočítáme vlastní vektory:

$$\lambda = 3\colon \begin{pmatrix} 2-3 & 4 & -3 \\ -1 & 10-3 & -6 \\ -1 & 8 & -4-3 \end{pmatrix} = \begin{pmatrix} -1 & 4 & -3 \\ -1 & 7 & -6 \\ -1 & 8 & -7 \end{pmatrix} \sim \begin{pmatrix} -1 & 4 & -3 \\ 0 & 3 & -3 \\ 0 & 4 & -4 \end{pmatrix} \sim \begin{pmatrix} -1 & 4 & -3 \\ 0 & 1 & -1 \end{pmatrix} \quad \text{vl v (}$$

$$\lambda = 2\colon \begin{pmatrix} 2-2 & 4 & -3 \\ -1 & 10-2 & -6 \\ -1 & 8 & -4-2 \end{pmatrix} = \begin{pmatrix} 0 & 4 & -3 \\ -1 & 8 & -6 \\ -1 & 8 & -6 \end{pmatrix} \sim \begin{pmatrix} -1 & 8 & -6 \\ 0 & 4 & -3 \end{pmatrix} \quad \begin{matrix} \text{vlastní} \\ \text{vektor:} \\ (0,3,4) \end{matrix}$$

Na rozdíl od předchozího příkladu vícenásobnému vlastnímu číslu 3 přísluší jen jeden lineárně nezávislý vlastní vektor. Tato matice má tedy dohromady jen dva lineárně nezávislé vlastní vektory: $(1,1,1), (0,3,4)$, které po řadě příslušejí vlastním číslům 3 a 2.

12.16. Poznámka. Vlastní číslo transformace $\mathcal{A}$ je podle věty ?? vlastním číslem všech matic této transformace (vzhledem k rozličným bázím). Dvě matice, které jsou maticemi stejné lineární transformace (jen vzhledem k různé bázi) budeme nazývat *podobné*. Následující věta ukazuje, jaký platí mezi podobnými maticemi vztah.

12.17. Věta. Nechť L je lineární prostor dimenze n a nechť (B) a (B') jsou nějaké jeho uspořádané báze. Nechť $\mathcal{A}\colon L \to L$ je lineární transformace a nechť $\mathbf{A}$ je její matice vzhledem

k bázi (B) a $\mathbf{B}$ je její matice vzhledem k bázi (B'). Pak existuje regulární matice $\mathbf{P} \in \mathbf{R}^{n,n}$ tak, že $\mathbf{B} = \mathbf{P}^{-1} \cdot \mathbf{A} \cdot \mathbf{P}$.

Důkaz. Označme $\mathbf{P} = \mathbf{P}_{B \to B'}$ matici přechodu od (B) k (B'). Podle věty ?? (vzorce třetího) platí $\mathcal{M}_{B'B'}(\mathcal{A}) = \mathbf{P}_{B' \to B} \cdot \mathcal{M}_{B,B}(\mathcal{A}) \cdot \mathbf{P}_{B \to B'}$. Protože $\mathbf{P}_{B' \to B} = (\mathbf{P}_{B \to B'})^{-1} = \mathbf{P}^{-1}$ (viz větu ??), dostáváme $\mathcal{M}_{B'B'}(\mathcal{A}) = \mathbf{P}^{-1} \cdot \mathcal{M}_{B,B}(\mathcal{A}) \cdot \mathbf{P}$, neboli $\mathbf{B} = \mathbf{P}^{-1} \cdot \mathbf{A} \cdot \mathbf{P}$.

12.18. Definice.* Matice $\mathbf{A}$ je *podobná* matici $\mathbf{B}$, pokud existuje regulární matice $\mathbf{P}$ taková, že platí $\mathbf{B} = \mathbf{P}^{-1} \cdot \mathbf{A} \cdot \mathbf{P}$.

12.19. Poznámka. Je-li $\mathbf{A}$ podobná $\mathbf{B}$, pak je i $\mathbf{B}$ podobná $\mathbf{A}$, protože místo matice $\mathbf{P}$ můžeme použít matici $\mathbf{P}^{-1}$. Stačí tedy říkat, že matice jsou si vzájemně podobné. Je-li $\mathbf{A}$ podobná $\mathbf{B}$ a $\mathbf{B}$ podobná $\mathbf{C}$, pak je $\mathbf{A}$ podobná $\mathbf{C}$, protože součin regulárních matic je matice regulární a protože $(\mathbf{PQ})^{-1} = \mathbf{Q}^{-1}\mathbf{P}^{-1}$. Matice je podobná sama sobě, protože $\mathbf{E}$ je regulární.

12.20. Poznámka. Protože podobné matice jsou matice stejné lineární transformace, jen vzhledem k případně různým bázím, mají samozřejmě všechny vzájemně podobné matice stejná vlastní čísla. V následující větě ukážeme, že mají i stejný charakteristický polynom.

12.21. Věta.* Podobné matice mají stejný charakteristický polynom.

Důkaz. Nechť $\mathbf{P}$ je regulární. Matice $\mathbf{P}^{-1}\mathbf{A}\mathbf{P}$ je podobná matici $\mathbf{A}$. Vypočteme její charakteristický polynom:

$$\begin{aligned}\det(\mathbf{P}^{-1}\mathbf{A}\mathbf{P} - \lambda\,\mathbf{E}) &= \det(\mathbf{P}^{-1}\mathbf{A}\mathbf{P} - \lambda\,\mathbf{P}^{-1}\mathbf{E}\mathbf{P}) = \det(\mathbf{P}^{-1}\mathbf{A}\mathbf{P} - \mathbf{P}^{-1}\lambda\,\mathbf{E}\mathbf{P}) = \\ &= \det(\mathbf{P}^{-1}\,(\mathbf{A} - \lambda\,\mathbf{E})\,\mathbf{P}) = \det\mathbf{P}^{-1}\,\det(\mathbf{A} - \lambda\,\mathbf{E})\,\det\mathbf{P} = \det(\mathbf{A} - \lambda\,\mathbf{E}),\end{aligned}$$

protože $\det\mathbf{P}^{-1}\det\mathbf{P} = 1$.

12.22. Poznámka. Matice z příkladů ?? a ?? mají sice stejný charakteristický polynom, ale za chvíli ukážeme, že si nejsou podobné. Tvrzení věty ?? tedy nelze obrátit.

12.23. Příklad. Diagonální matice

$$\mathbf{D} = \begin{pmatrix} \lambda_1 & 0 & 0 & \dots & 0 \\ 0 & \lambda_2 & 0 & \dots & 0 \\ 0 & 0 & \lambda_3 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

má charakteristický polynom $(\lambda_1 - \lambda)\,(\lambda_2 - \lambda)\cdots(\lambda_n - \lambda)$, protože determinant diagonální matice $\mathbf{D} - \lambda\,\mathbf{E}$ je roven součinu prvků na diagonále. Vlastní čísla matice $\mathbf{D}$ tedy jsou $\lambda_1, \lambda_2, \dots, \lambda_n$.

Vlastní vektor matice $\mathbf{D}$ příslušný vlastnímu číslu λ_i je vektor obsahující samé nuly s výjimkou i-té složky, ve které je nějaké nenulové číslo, třeba jednička.

Matici $\mathbf{D}$ z tohoto příkladu budeme značit $\mathbf{D} = \mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$. Tím ušetříme papír.

12.24. Věta. Nechť $\mathbf{A}$ je čtvercová matice typu (n, n). Sestavme libovolná komplexní čísla $\lambda_1, \ldots, \lambda_n$ do diagonální matice $\mathbf{D} = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ a libovolné nenulové vektory $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ z $\mathbf{C}^n$ zapišme do sloupců matice $\mathbf{P}$, tj. $\mathbf{P} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$. Pak platí: čísla $\lambda_1, \ldots, \lambda_n$ jsou vlastními čísly matice $\mathbf{A}$ a $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ jsou jejich odpovídající vlastní vektory právě tehdy, když je splněna rovnost $\mathbf{PD} = \mathbf{AP}$.

Důkaz. Rozepišme maticové násobení: $\mathbf{PD} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) \cdot \mathrm{diag}(\lambda_1, \ldots, \lambda_n) = (\lambda_1 \boldsymbol{x}_1, \ldots, \lambda_n \boldsymbol{x}_n)$. Dále je $\mathbf{AP} = \mathbf{A}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) = (\mathbf{A}\boldsymbol{x}_1, \ldots, \mathbf{A}\boldsymbol{x}_1)$. Máme tedy obě strany zkoumané rovnosti $\mathbf{PD} = \mathbf{AP}$ rozepsány do sloupců. Vidíme, že rovnost v i-tém sloupci $\lambda_i \boldsymbol{x}_i = \mathbf{A}\boldsymbol{x}_i$ platí právě tehdy, když λ_i je vlastní číslo matice $\mathbf{A}$ a $\boldsymbol{x}_i$ je příslušný vlastní vektor.

12.25. Věta. Nechť má čtvercová matice $\mathbf{A}$ s n řádky n lineárně nezávislých vlastních vektorů (každý z nich přísluší nějakému vlastnímu číslu matice). Pak je matice $\mathbf{A}$ podobná diagonální matici.

Důkaz. Sestavíme diagonální matici $\mathbf{D}$ z vlastních čísel příslušných vlastním vektorům $\boldsymbol{x}_1, \ldots, \boldsymbol{x}$
Dále použijeme předchozí větu. Protože matice $\mathbf{P} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ obsahuje podle předpokladu

věty lineárně nezávislé sloupce, je $\mathbf{P}$ regulární, takže je možné vztah $\mathbf{PD} = \mathbf{AP}$ vynásobit zprava maticí $\mathbf{P}^{-1}$. Dostáváme $\mathbf{A} = \mathbf{PDP}^{-1}$, takže matice $\mathbf{A}$ je podobná matici $\mathbf{D}$.

12.26. Věta.* Nechť je matice $\mathbf{A}$ podobná diagonální matici, to znamená, že existuje regulární matice $\mathbf{P}$ a diagonální matice $\mathbf{D}$ takové, že $\mathbf{A} = \mathbf{PDP}^{-1}$. Pak $\mathbf{D}$ obsahuje vlastní čísla matice $\mathbf{A}$ a ve sloupcích matice $\mathbf{P}$ jsou vlastní vektory příslušné (podle pořadí) odpovídajícím vlastním číslům zapsaným v $\mathbf{D}$.

Důkaz. Po převedení vztahu $\mathbf{A} = \mathbf{PDP}^{-1}$ na $\mathbf{AP} = \mathbf{PD}$ stačí použít větu ??.

12.27. Příklad. Matice z příkladu ?? má tři řádky a tři lineárně nezávislé vlastní vektory. Jsou tedy splněny předpoklady věty ?? a matice je podobná diagonální matici. Věta ?? nám dává návod, jak najít matici $\mathbf{P}$ a diagonální matici. Sestavíme vlastní vektory $(1,1,0), (-1,0,1), ($ do sloupců a dostáváme matici $\mathbf{P}$. Sestavíme v odpovídajícím pořadí vlastní čísla do diagonální matice, a dostáváme matici $\mathbf{D}$, pro kterou platí $\mathbf{A} = \mathbf{PDP}^{-1}$. Konkrétně:

$$\mathbf{A} = \begin{pmatrix} 5 & -2 & 2 \\ -1 & 4 & -1 \\ -4 & 4 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 & -2 \\ 1 & 0 & 1 \\ 0 & 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & -2 \\ 1 & 0 & 1 \\ 0 & 1 & 4 \end{pmatrix}^{-1}.$$

12.28. Příklad. Matice z příkladu ?? nemá tolik lineárně nezávislých vlastních vektorů, jako je počet jejích řádků. To znamená, že není podobná diagonální matici (kdyby byla, pak dostaneme spor s větou ??. Protože matice z příkladu ?? je podobná diagonální matici, zatímco matice z příkladu ?? není, nejsou si tyto matice ani vzájemně podobné.

12.29. Věta. Vlastní vektory, které příslušejí vzájemně různým vlastním číslům, jsou lineárně nezávislé.

Důkaz. Jeden vlastní vektor je samozřejmě lineárně nezávislý, protože je podle definice nenulový. Dále postupujeme indukcí. Přepokládáme, že matice $\mathbf{A}$ má lineárně nezávislé vlastní vektory $\boldsymbol{x}_1, \dots \boldsymbol{x}_k$ příslušející různým vlastním číslům $\lambda_1, \dots, \lambda_k$ a přidáme do této skupiny vlastní vektor $\boldsymbol{x}_{k+1}$ příslušející zatím nepoužitému vlastnímu číslu λ_{k+1}. Předpokládáme rovnost $\sum_{i=1}^{k+1} \alpha_i \boldsymbol{x}_i = \boldsymbol{o}$ a ukážeme, že všechny koeficienty α_i musejí být nulové. Tím dokážeme lineární nezávislost. Vektory v uvedené rovnosti píšeme do sloupců a rovnost vynásobíme zleva maticí $\mathbf{A} - \lambda_{k+1}\mathbf{E}$. Dostáváme:

$$(\mathbf{A}-\lambda_{k+1}\mathbf{E}) \sum_{i=1}^{k+1} \alpha_i \boldsymbol{x}_i = \sum_{i=1}^{k+1} \alpha_i (\mathbf{A}\boldsymbol{x}_i - \lambda_{k+1}\boldsymbol{x}_i) = \sum_{i=1}^{k+1} \alpha_i (\lambda_i \boldsymbol{x}_i - \lambda_{k+1}\boldsymbol{x}_i) = \sum_{i=1}^{k+1} \alpha_i (\lambda_i - \lambda_{k+1})\, \boldsymbol{x}_i = \boldsymbol{o}$$

Koeficient u posledního sčítance v této rovnosti je nulový, protože $\lambda_{k+1} - \lambda_{k+1} = 0$. Podle indukčního předpokladu jsou vektory $\boldsymbol{x}_1, \dots \boldsymbol{x}_k$ lineárně nezávislé, takže i ostatní koeficienty

musejí být nulové. Protože ale $\lambda_i \neq \lambda_{k+1}$, musí $\alpha_i = 0$ pro $i \in \{1, \dots, k\}$. Dosadíme-li tento poznatek do výchozího tvaru rovnosti, máme $0\,\boldsymbol{x}_1 + \cdots + 0\,\boldsymbol{x}_k + \alpha_{k+1}\boldsymbol{x}_{k+1} = \alpha_{k+1}\boldsymbol{x}_{k+1} = \boldsymbol{o}$. Protože $\boldsymbol{x}_{k+1}$ je vlastní vektor a tudíž nenulový, musí $\alpha_{k+1} = 0$.

12.30. Poznámka. Nechť $\mathbf{A}$ je typu (n, n) a nechť jsou všechna vlastní čísla matice $\mathbf{A}$ jednonásobná. To znamená, že existuje n různých vlastních čísel. Pak podle předchozí věty jim příslušející vlastní vektory jsou lineárně nezávislé. Podle věty ?? je tedy matice $\mathbf{A}$ podobná diagonální matici.

12.31. Poznámka. Má-li matice $\mathbf{A}$ vícenásobná vlastní čísla, pak se může stát, že je podobná s diagonální maticí. Záleží na tom, zda se povede najít n lineárně nezávislých vlastních vektorů. Vzhledem k tomu, že vlastní vektory leží v nulových prostorech matic $\mathbf{A} - \lambda\mathbf{E}$ (kde λ je vlastní číslo), půjde o to, jakou mají tyto prostory dimenzi. Odpověď na to dávají následující věty.

12.32. Věta. Jestliže $\mathbf{A}$ a $\mathbf{B}$ jsou podobné matice, pak $\dim \mathrm{Null}(\mathbf{A} - \lambda\mathbf{E}) = \dim \mathrm{Null}(\mathbf{B} - \lambda\mathbf{E})$.

Důkaz. Protože $\dim \mathrm{Null}(\mathbf{A} - \lambda\mathbf{E}) = n - \mathrm{hod}(\mathbf{A} - \lambda\mathbf{E})$, kde n je počet řádků matice $\mathbf{A}$, stačí dokázat, že $\mathrm{hod}(\mathbf{A} - \lambda\mathbf{E}) = \mathrm{hod}(\mathbf{B} - \lambda\mathbf{E})$. Z věty ?? víme, že platí:

$$\mathrm{hod}(\mathbf{B} - \lambda\mathbf{E}) = \mathrm{hod}(\mathbf{P}^{-1}\mathbf{A}\mathbf{P} - \lambda\mathbf{P}^{-1}\mathbf{E}\mathbf{P}) = \mathrm{hod}(\mathbf{P}^{-1}(\mathbf{A} - \lambda\mathbf{E})\mathbf{P}) = \mathrm{hod}(\mathbf{A} - \lambda\mathbf{E})$$

12.33. Věta. Nechť λ_i je k-násobné vlastní číslo matice $\mathbf{A}$ a nechť d je dimenze nulového prostoru matice $\mathbf{A} - \lambda_i\mathbf{E}$. Pak $d \leq k$.

Důkaz. V nulovém prostoru matice $\mathbf{A}-\lambda_i\mathbf{E}$ můžeme najít bázi, která má d vektorů: $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_d$ a doplníme ji na bázi prostoru $\mathbf{C}^n$: $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_d, \ldots, \boldsymbol{b}_n)$. Nechť $\mathcal{A}\colon \mathbf{C}^n \to \mathbf{C}^n$ je transformace definována vzorcem $\mathcal{A}(\boldsymbol{x}) = \mathbf{A}\boldsymbol{x}$ a nechť $\mathbf{B}$ je matice této transformace vzhledem k bázi (B). Je zřejmé, že matice $\mathbf{A}$ a $\mathbf{B}$ jsou si vzájemně podobné, protože jsou to matice stejné lineární transformace. Zvolme $\boldsymbol{b}_j$ z báze (B) pro $j \leq d$. Souřadnice tohoto vektoru vzhledem k bázi (B) označme $\boldsymbol{y}_j$. Tyto souřadnice obsahují jedinou jedničku v j-té složce, jinak nuly. Platí $\mathbf{B}\boldsymbol{y}_j = \lambda_i\boldsymbol{y}_j$, takže j-tý sloupec matice $\mathbf{B}$ je roven j-tému sloupci matice $\lambda_i\mathbf{E}$. Matice $\mathbf{B}$ má tedy následující blokový tvar (první blok je čtvercový s d řádky a sloupci):

$$\mathbf{B} = \begin{pmatrix} \lambda_i\mathbf{E} & \mathbf{B}' \\ \mathbf{O} & \mathbf{C} \end{pmatrix}, \quad \text{tj.} \quad p(\lambda) = \det(\mathbf{B} - \lambda\mathbf{E}) = \det \begin{pmatrix} (\lambda_i - \lambda)\,\mathbf{E} & \mathbf{B}' \\ \mathbf{O} & \mathbf{C}' \end{pmatrix} = (\lambda_i - \lambda)^d \det(\mathbf{C}'),$$

takže λ_i je aspoň d-násobným kořenem charakteristického polynomu matice $\mathbf{B}$, tj. podle věty ?? je aspoň d-násobným kořenem charakteristického polynomu matice $\mathbf{A}$.

12.34. Věta. Nechť λ je vlastní číslo matice $\mathbf{A}$. Nechť N_1 je lineárně nezávislá množina vlastních vektorů, které nepříslušejí vlastnímu číslu λ a dále N_2 je lineárně nezávislá množina vlastních vektorů, které příslušejí vlastnímu číslu λ. Pak množina $N_1 \cup N_2$ je lineárně nezávislá.

Důkaz. Označme $N_1 = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k\}$ a $N_2 = \{\boldsymbol{x}_{k+1}, \ldots, \boldsymbol{x}_m\}$. Lineární nezávislost množiny vektorů $N_1 \cup N_2 = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m\}$ se ověří stejně jako v důkazu věty ??. Lineární kombinaci těchto vektorů, kterou položíme rovnu nulovému vektoru, násobíme zleva maticí $\mathbf{A} - \lambda\mathbf{E}$. Tím zjistíme, že koeficienty u vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k$ musejí být nulové. Konečně kvůli tomu, že N_2 je lineárně nezávislá, dostáváme nulové koeficienty i u vektorů $\boldsymbol{x}_{k+1}, \ldots, \boldsymbol{x}_m$.

12.35. Věta.* Matice $\mathbf{A}$ je podobná s diagonální maticí právě tehdy, když pro každé vlastní číslo λ_i násobnosti k_i platí $\dim \mathrm{Null}(\mathbf{A} - \lambda_i\mathbf{E}) = k_i$.

Důkaz. Nechť $\mathbf{A}$ typu (n, n) je podobná s diagonální maticí. Pak $\mathbf{P}$ ve vzorci $\mathbf{AP} = \mathbf{PD}$ musí být regulární. V matici $\mathbf{P}$ jsou ve sloupcích vlastní vektory, takže musí existovat n lineárně nezávislých vlastních vektorů. Podle věty ?? můžeme z každého nulového prostoru matice $\mathbf{A} - \lambda_i\mathbf{E}$ vybrat maximálně k_i lineárně nezávislých vektorů. Jinde se vlastní vektory nenalézají. Abychom získali n lineárně nezávislých vlastních vektorů, je třeba z každého nulového prostoru matice $\mathbf{A} - \lambda_i\mathbf{E}$ vzít právě k_i lineárně nezávislých vektorů, takže $\dim \mathrm{Null}(\mathbf{A} - \lambda_i\mathbf{E}) = k_i$.

Nechť obráceně $\dim \mathrm{Null}(\mathbf{A} - \lambda_i\mathbf{E}) = k_i$. Z každého nulového prostoru vybereme k_i lineárně nezávislých vektorů. Množina všech takto vybraných vektorů je podle věty ?? lineárně nezávislá, takže jimi sestavená matice $\mathbf{P}$ je regulární a je možné ze vzorce $\mathbf{AP} = \mathbf{PD}$ přejít na $\mathbf{A} = \mathbf{PDP}^{-1}$.

12.36. Poznámka. Stále předpokládáme čtvercovou matici $\mathbf{A}$ typu (n, n). Jestliže $\dim \mathrm{Null}(\mathbf{A} - \lambda_i \mathbf{E})$ je menší než násobnost vlastního čísla λ_i, pak $\mathbf{A}$ není podobná s diagonální maticí. Příklad ?? ilustruje, že takové případy opravdu nastávají. Matice $\mathbf{A}$ je pak podobná jen „skoro diagonální matici“, která má na hlavní diagonále vlastní čísla a těsně nad touto diagonálou se občas vyskytují jedničky. Této matici se říká *Jordanův kanonický tvar*. Je potřeba definovat tzv. *zobecněný vlastní vektor* a tento pojem použít k vybudování regulární matice $\mathbf{P}$, která převádí matici $\mathbf{A}$ na Jordanův kanonický tvar. Všechny tyto pojmy vyžadují hlubší studium a přesahují bohužel rámec tohoto úvodního textu. Pro další studium lze doporučit [16].

12.37. Poznámka. Věty ?? a ?? se dají formulovat z úhlu pohledu lineární transformace:

12.38. Věta. Nechť $\mathcal{A}\colon L \to L$ je lineární transformace, $\dim L = n$. Transformace $\mathcal{A}$ má n lineárně nezávislých vlastních vektorů právě tehdy, když existuje báze (B) prostoru L taková, že $\mathcal{A}$ má vzhledem k této bázi diagonální matici $\mathbf{D}$. Přitom na diagonále matice $\mathbf{D}$ jsou vlastní čísla transformace $\mathcal{A}$ a báze (B) obsahuje vlastní vektory příslušné vlastním číslům v matici $\mathbf{D}$ ve stejném pořadí.

Důkaz. Zvolme nějakou výchozí bázi (V) prostoru L. Označme symbolem $\mathbf{A}$ matici transformace $\mathcal{A}$ vzhledem k bázi (V). Existence báze (B) takové, že matice transformace $\mathcal{A}$ vzhledem k ní je $\mathbf{D}$, je ekvivalentní s platností vztahu $\mathbf{A} = \mathbf{P}\mathbf{D}\mathbf{P}^{-1}$, kde $\mathbf{P}$ je matice přechodu od (V) k (B). Dále při důkazu tvrzení „právě tehdy když“ použijeme v jednom směru větu ??. V

druhém směru použijeme větu ?? a skutečnost, že matice přechodu $\mathbf{P}$ obsahuje ve sloupcích souřadnice báze (B) vzhledem k bázi (V).

12.39. Poznámka. Při práci s lineární transformací se někdy hodí zvolit takovou bázi, ve které je matice této transformace „co nejbližší“ matici diagonální. Právě vyslovená věta říká, že za jistých okolností lze zvolit bázi, vzhledem ke které je matice transformace přímo diagonální. Pak můžeme na danou transformaci pohlížet jen jako na transformaci změny měřítka (λ_1 krát první souřadnice, λ_2 krát druhá souřadnice, atd. až λ_n krát poslední souřadnice).

12.40. Poznámka. Nechť dimenze L je rovna n a vraťme se k představě vlastních vektorů jako směrových vektorů přímek, které lineární transformace nechává beze změny (viz motivační příklady v úvodu této kapitoly). Povede-li se najít n různých přímek, které transformace $\mathcal{A}$ ponechává beze změny, pak jejich směrové vektory tvoří bázi, vzhledem ke které má transformace $\mathcal{A}$ diagonální matici.

12.41. Shrnutí. Definovali jsme vlastní číslo a vlastní vektory transformace /??/. Vlastní vektor je směrový vektor přímky, kterou nechává transformace beze změny a vlastní číslo je koeficient změny měřítka ve směru vlastního vektoru. Vlastní číslo transformace je vlastním číslem každé její matice, třebaže jsou to matice vzhledem k různým bázím /??, ??/.

Vlastní čísla počítáme jako kořeny chrakteristického polynomu $\det(\mathbf{A} - \lambda\mathbf{E})$ /??/.

Dvě matice stejné transformace vzhledem k různým bázím se nazývají podobné /??/. Mají stejný charakteristický polynom /??/.

Podobnost s diagonální maticí je zaručena pro matice se vzájemně různými vlastními čísly /??/. Ovšem i některé matice s násobnými vlastními čísly jsou podobné s diagonální, ale ne všechny.

Je-li $\mathbf{D}$ diagonální matice, se kterou je podobná matice $\mathbf{A}$, pak $\mathbf{D}$ obsahuje vlastní čísla matice $\mathbf{A}$ a sestavíme-li do sloupců matice $\mathbf{P}$ vlastní vektory odpovídající vlastním číslům $\mathbf{A}$, pak $\mathbf{A} = \mathbf{PDP}^{-1}$.

13. Lineární prostory se skalárním součinem

13.1. Poznámka. Lineární prostor je libovolná množina, na které je definováno sčítání a násobení konstantou tak, aby byly splněny vlastnosti (1) až (7) z definice ??. Pokud na takové množině navíc definujeme násobení prvků *mezi sebou* tak, že výsledek násobení je reálné číslo a násobení splňuje níže uvedené vlastnosti (1) až (4), definovali jsme na lineárním prostoru skalární součin. Ten nám umožní pracovat s novými vlastnostmi prvků lineárního prostoru, jako je jejich velikost a úhel mezi dvěma prvky.

13.2. Definice.* Nechť L je lineární prostor. Operaci $\cdot\colon L \times L \to \mathbf{R}$ nazveme *skalárním součinem*, pokud splňuje $\forall \boldsymbol{x} \in L$, $\forall \boldsymbol{y} \in L$, $\forall \boldsymbol{z} \in L$, $\forall \alpha \in \mathbf{R}$ následující vlastnosti

$$
\begin{aligned}
&(1) \quad \boldsymbol{x} \cdot \boldsymbol{y} = \boldsymbol{y} \cdot \boldsymbol{x},\\
&(2) \quad (\boldsymbol{x} + \boldsymbol{y}) \cdot \boldsymbol{z} = \boldsymbol{x} \cdot \boldsymbol{z} + \boldsymbol{y} \cdot \boldsymbol{z},\\
&(3) \quad (\alpha \cdot \boldsymbol{x}) \cdot \boldsymbol{y} = \alpha \cdot (\boldsymbol{x} \cdot \boldsymbol{y}),\\
&(4) \quad \boldsymbol{x} \cdot \boldsymbol{x} \geq 0, \quad \boldsymbol{x} \cdot \boldsymbol{x} = 0 \text{ jen tehdy, když } \boldsymbol{x} = \boldsymbol{o}.
\end{aligned}
$$

Ve vlastnosti (4) značí symbol $\boldsymbol{o}$ nulový vektor lineárního prostoru L.

Lineární prostor L, na kterém je definován skalární součin, nazýváme *lineárním prostorem se skalárním součinem*.

13.3. Poznámka. Je třeba rozlišovat mezi podobně znějícími pojmy „skalární násobek“ a „skalární součin“. Skalární násobek $\cdot : \mathbf{R} \times L \to L$ je násobek vektoru reálným číslem, který je definován v každém lineárním prostoru. Na druhé straně skalární součin $\cdot : L \times L \to \mathbf{R}$ je součin vektorů mezi sebou.

13.4. Poznámka. Upozorňujeme, že stejně jako v definici lineárního prostoru ??, jsou ve vlastnostech (1) až (4) definice skalárního součinu používány symboly „+“ a „$\cdot$“ v různých významech podle toho, jakého typu jsou jejich operandy. Například první „+“ ve vlastnosti (2) označuje sčítání vektorů podle definice lineárního prostoru, zatímco druhé „+“ v této vlastnosti je sčítáním reálných čísel. Nebo první symbol „$\cdot$“ ve vlastnosti (3) znamená skalární násobek definovaný v lineárním prostoru L, druhý symbol „$\cdot$“ označuje skalární součin. Třetí symbol „$\cdot$“ ve vlastnosti (3) je součin reálných čísel a poslední symbol „$\cdot$“ v této vlastnosti znovu znamená skalární součin.

Dále připomínáme, že budeme symbol „$\cdot$“ jako dosud často vynechávat, takže místo $\boldsymbol{x} \cdot \boldsymbol{y}$ budeme stručně psát $\boldsymbol{xy}$.

13.5. Poznámka. Všimneme si, že jsme v definici ?? lineárního prostoru definovali tento prostor „nad reálnými čísly“, protože jsme definovali násobek vektoru *reálným číslem*. Nic nám ale nebránilo zcela stejně definovat násobek vektoru komplexním číslem. Až dosud jsme mohli nahradit slovo „reálné číslo“ slovem „komplexní číslo“ a naše teorie by zůstala platná. Všechny předchozí věty by nadále platily.

Kdybychom ale chtěli definovat skalární součin jako komplexní číslo, museli bychom upravit vlastnost (1) definice ?? takto:

$$(1) \quad \boldsymbol{xy} = \overline{\boldsymbol{yx}},$$

kde pruh nad komplexním číslem $\boldsymbol{yx}$ značí komplexně sdružené číslo. Některá tvrzení se tedy budou v případě komplexního skalárního součinu nepatrně lišit od tvrzení, která níže dokážeme. Protože se většina čtenářů tohoto textu nachází zatím v prvním semestru a nemá za sebou analýzu komplexních čísel, zjednodušíme si život tím, že zůstaneme u reálných čísel. Pro odvození důležitých vlastností lineárních prostorů se skalárním součinem nám to bude stačit. Zájemce o důsledky definice komplexního skalárního součinu odkážeme například na učebnici [5].

13.6. Věta. Nechť L je lineární prostor se skalárním součinem, $\boldsymbol{o}$ je jeho nulový vektor. Pak pro všechna $\boldsymbol{x} \in L$, $\boldsymbol{y} \in L$ a $\boldsymbol{z} \in L$ platí: (1) $\boldsymbol{x} \cdot \boldsymbol{o} = \boldsymbol{o} \cdot \boldsymbol{x} = 0$, (2) $\boldsymbol{z} \cdot (\boldsymbol{x} + \boldsymbol{y}) = \boldsymbol{zx} + \boldsymbol{zy}$.

Důkaz. První vlastnost plyne z vlastnosti (7) definice lineárního prostoru ?? a z vlastnosti (3) definice skalárního součinu ??. Platí $(0\boldsymbol{y}) \cdot \boldsymbol{x} = 0 \cdot \boldsymbol{xy} = 0$

Druhá vlastnost plyne z komutativity skalárního součinu, tj. z vlastnosti (1) definice ?? a dále z vlastnosti (2) této definice.

13.7. Příklad. Pro $\boldsymbol{x} \in \mathbf{R}^n$, $\boldsymbol{y} \in \mathbf{R}^n$, $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$, $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$ definujme

$$\boldsymbol{x} \cdot \boldsymbol{y} = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n. \tag{13.1}$$

Ukážeme, že takto definovaný součin vektorů $\boldsymbol{x}$ a $\boldsymbol{y}$ je skalárním součinem. Je $\boldsymbol{x} \cdot \boldsymbol{y} \in \mathbf{R}$. Nechť ještě $\boldsymbol{z} \in \mathbf{R}^n$, $\boldsymbol{z} = (z_1, z_2, \ldots, z_n)$ a $\alpha \in \mathbf{R}$. Ověříme postupně vlastnosti (1) až (4):

(1) $\boldsymbol{x} \cdot \boldsymbol{y} = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n = y_1 x_1 + y_2 x_2 + \cdots + y_n x_n = \boldsymbol{y} \cdot \boldsymbol{x}$,

(2) $(\boldsymbol{x} + \boldsymbol{y}) \cdot \boldsymbol{z} = (x_1 + y_1)\, z_1 + (x_2 + y_2)\, z_2 + \cdots + (x_n + y_n)\, z_n =$
$= x_1 z_1 + x_2 z_2 + \cdots + x_n z_n + y_1 z_1 + y_2 z_2 + \cdots + y_n z_n = \boldsymbol{x} \cdot \boldsymbol{z} + \boldsymbol{y} \cdot \boldsymbol{z}$,

(3) $(\alpha \cdot \boldsymbol{x}) \cdot \boldsymbol{y} = \alpha x_1 y_1 + \alpha x_2 y_2 + \cdots + \alpha x_n y_n = \alpha\,(x_1 y_1 + x_2 y_2 + \cdots + x_n y_n) = \alpha\,(\boldsymbol{x} \cdot \boldsymbol{y})$,

(4) $\boldsymbol{x} \cdot \boldsymbol{x} = x_1^2 + x_2^2 + \cdots + x_n^2 \geq 0$.

Vidíme, že z $x_1^2 + x_2^2 + \cdots + x_n^2 = 0$ plyne $x_1 = x_2 = \cdots = x_n = 0$, takže je splněna i druhá část vlastnosti (4).

Skalární součin na $\mathbf{R}^n$ definovaný vzorcem (13.1) nazýváme *standardním skalárním součinem*. Následující příklady ukazují, že existují i jiné skalární součiny na $\mathbf{R}^n$.

13.8. Příklad. Definujme součin na $\mathbf{R}^2$ takto

$$(x_1, x_2) \cdot (y_1, y_2) = x_1 y_1 + 6 x_2 y_2 + 2 x_1 y_2 + 2 x_2 y_1.$$

Ukážeme, že takto definovaný součin je skalárním součinem na $\mathbf{R}^2$.

Ověříme vlastnosti (1) až (4) definice ??

(1) $(x_1, x_2) \cdot (y_1, y_2) = x_1y_1 + 6x_2y_2 + 2x_1y_2 + 2x_2y_1 =$
$= y_1x_1 + 6y_2x_2 + 2y_1x_2 + 2y_2x_1 = (y_1, y_2) \cdot (x_1, x_2),$

(2) $\big((x_1, x_2) + (y_1, y_2)\big) \cdot (z_1, z_2) = (x_1 + y_1)\, z_1 + 6(x_2 + y_2)\, z_2 + 2(x_1 + y_1)\, z_2 + 2(x_2 + y_2)\, z_1$
$= x_1z_1 + 6x_2z_2 + 2x_1z_2 + 2x_2z_1 + y_1z_1 + 6y_2z_2 + 2y_1z_2 + 2y_2z_1 =$
$= (x_1, x_2) \cdot (z_1, z_2) + (y_1, y_2) \cdot (z_1, z_2),$

(3) $\big(\alpha\,(x_1, x_2)\big) \cdot (y_1, y_2) = (\alpha\, x_1, \alpha\, x_2) \cdot (y_1, y_2) = \alpha x_1y_1 + 6\alpha x_2y_2 + 2\alpha x_1y_2 + 2\alpha x_2y_1 =$
$= \alpha\,(x_1y_1 + 6x_2y_2 + 2x_1y_2 + 2x_2y_1) = \alpha\,\big((x_1, x_2) \cdot (y_1, y_2)\big),$

(4) $(x_1, x_2) \cdot (x_1, x_2) = x_1^2 + 6x_2^2 + 4x_1x_2 \overset{?}{\geq} 0.$

Abychom dokázali vlastnost (4), potřebujeme pro $x_1 \neq 0$, $x_2 \neq 0$ dokázat, že $x_1^2 + 6x_2^2 + 4x_1x_2 > 0$. Nechť $a = x_2/x_1$, tj. $x_2 = ax_1$. Po dosazení je $x_1^2 + 6a^2x_1^2 + 4ax_1^2 = x_1^2(1 + 6a^2 + 4a)$. Aby byl daný výraz větší než nula, stačí aby $6a^2 + 4a + 1 > 0$, $\forall a \in \mathbf{R}$. Protože diskriminant této kvadratické nerovnice je roven $D = 16 - 24 = -8 < 0$, je nerovnost $6a^2 + 4a + 1 > 0$ splněna pro všechna $a \in \mathbf{R}$.

13.9. Příklad. Ukážeme, že předpis $(x_1, x_2) \circ (y_1, y_2) = x_1y_1 + 2x_2y_2 + 2x_1y_2 + 2x_2y_1$ není skalárním součinem. Vlastnosti (1) až (3) jsou zřejmě splněny. Není splněna vlastnost (4), protože například

$$(-1, 1) \circ (-1, 1) = 1 + 2 - 2 - 2 = -1 \not> 0.$$

13.10. Poznámka. Výše uvedené příklady nás vedou k otázce, jak charakterizovat všechny skalární součiny na $\mathbf{R}^n$ a jak je rychle poznat. Souvisí to s tzv. pozitivně definitními a symetrickými maticemi. Níže uvádím nejdůležitější výsledky z této oblasti jen pro čtenáře, který chce být lépe informován. Nám ostatním bude v dalším textu stačit existence standardního skalárního součinu na $\mathbf{R}^n$ a povědomí, že existují i jiné skalární součiny. Téma symetrických a pozitivně definitních matic je možno přeskočit a věnovat se rovnou definici velikosti vektoru ??.

13.11. Definice. Čtvercová matice $\mathbf{A} \in \mathbf{R}^{n,n}$ je *symetrická*, pokud platí $\mathbf{A}^T = \mathbf{A}$.

13.12. Definice. Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$ je čtvercová matice. Označme $\mathbf{A}_i \in \mathbf{R}^{n-i,n-i}$ čtvercovou matici, která vzniká z matice $\mathbf{A}$ vynecháním posledních i řádků a posledních i sloupců. Matice $\mathbf{A}$ se nazývá *pozitivně definitní*, pokud všechny determinanty $\det \mathbf{A}_i$, $i \in \{0, 1, 2, \ldots, n-1\}$ jsou kladné.

13.13. Poznámka. Pozitivně definitní matice je vždy regulární, protože $\det \mathbf{A} = \det \mathbf{A}_0 > 0$.

13.14. Věta. Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$ je čtvercová matice. Definujme součin na $\mathbf{R}^n$ takto. Pro $\boldsymbol{x} \in \mathbf{R}^n$, $\boldsymbol{y} \in \mathbf{R}^n$ je

$$\boldsymbol{x} \cdot \boldsymbol{y} = \boldsymbol{x} \cdot \mathbf{A} \cdot \boldsymbol{y}^T,$$

kde na pravé straně rovnosti je maticový součin jednořádkové matice $\boldsymbol{x}$, která obsahuje složky vektoru $\boldsymbol{x}$, s maticí $\mathbf{A}$ a s maticí $\boldsymbol{y}^T$, což je sloupec složek vektoru $\boldsymbol{y}$.

Pak $\boldsymbol{x} \cdot \boldsymbol{y}$ je skalárním součinem právě tehdy, když $\mathbf{A}$ je symetrická a pozitivně definitní matice.

Důkaz. Uvedeme jen stručný náznak. Pro vlastnost (1) skalárního součinu je nutná symetrie matice $\mathbf{A}$. Vlastnost (2) a (3) je zaručena pro jakoukoli čtvercovou matici $\mathbf{A}$. Konečně vlastnost (4) je zaručena díky tomu, že matice $\mathbf{A}$ je pozitivně definitní. Na oprávněnou otázku „proč“ zde máme malý prostor pro odpověď. Odkazujeme například na učebnici [5].

13.15. Příklad. Vraťme se k příkladu ??. Tam je skalární součin definován takto:

$$\boldsymbol{x} \cdot \boldsymbol{y} = (x_1, x_2) \cdot \begin{pmatrix} 1 & 2 \\ 2 & 6 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

Protože pro uvedenou matici platí $\mathbf{A} = \mathbf{A}^T$, jedná se o symetrickou matici. Spočteme dále jednotlivé determinanty: $\det \mathbf{A}_0 = \det \mathbf{A} = 2$, $\det \mathbf{A}_1 = \det(1) = 1$. Protože oba determinanty jsou kladná čísla, jedná se o pozitivně definitní matici. Podle věty ?? je definovaný součin skalárním součinem.

13.16. Poznámka. Budeme definovat velikost vektoru a úhel mezi dvěma nenulovými vektory na obecných lineárních prostorech se skalárním součinem. Tyto pojmy definujeme jen pomocí skalárního součinu pro zcela libovolné vektory. V následující kapitole ukážeme, že pokud budeme pracovat s vektory s geometrickým významem (např. s orientovanými úsečkami), pak pojmy velikost a úhel nyní zavedené abstraktně budou znamenat přesně to, co od nich z geometrického hlediska očekáváme.

13.17. Definice.* Nechť L je lineární prostor se skalárním součinem. Pro $\boldsymbol{x} \in L$ definujeme *velikost vektoru* $\boldsymbol{x}$ hodnotou $\sqrt{\boldsymbol{x} \cdot \boldsymbol{x}}$. Velikost vektoru $\boldsymbol{x}$ značíme $\|\boldsymbol{x}\|$, takže je

$$\|\boldsymbol{x}\| = \sqrt{\boldsymbol{x} \cdot \boldsymbol{x}}, \qquad \text{tj.} \quad \|\boldsymbol{x}\|^2 = \boldsymbol{x} \cdot \boldsymbol{x}.$$

Místo pojmu „velikost vektoru“ se často používá pojem *norma vektoru*.

13.18. Poznámka. Vidíme, že velikost je nezáporné číslo a že každý vektor má svou velikost. To nám zaručuje vlastnost (4) definice ??. Je $\boldsymbol{x} \cdot \boldsymbol{x} \geq 0$, takže odmocnina z tohoto čísla je definována.

Dále vidíme, že jedině nulový vektor má velikost rovnu nule a žádný jiný. To nám zaručuje druhá část vlastnosti (4).

13.19. Věta. Nechť $\boldsymbol{x}$ je prvkem lineárního prostoru se skalárním součinem, $\alpha \in \mathbf{R}$. Pak

$$\|\alpha\,\boldsymbol{x}\| = |\alpha| \cdot \|\boldsymbol{x}\|.$$

Důkaz. $\|\alpha\,\boldsymbol{x}\| = \sqrt{(\alpha\,\boldsymbol{x}) \cdot (\alpha\,\boldsymbol{x})} = \sqrt{\alpha^2\,\boldsymbol{x} \cdot \boldsymbol{x}} = \sqrt{\alpha^2} \cdot \sqrt{\boldsymbol{x} \cdot \boldsymbol{x}} = |\alpha| \cdot \|\boldsymbol{x}\|.$

13.20. Definice* Nechť L je lineární prostor se skalárním součinem a $\boldsymbol{x} \in L$, $\boldsymbol{y} \in L$, $\boldsymbol{x} \neq \boldsymbol{o}$, $\boldsymbol{y} \neq \boldsymbol{o}$. Pak *úhel mezi vektory* $\boldsymbol{x}$ *a* $\boldsymbol{y}$ je takové číslo $\varphi \in \langle 0, \pi)$, pro které platí

$$\cos\varphi = \frac{\boldsymbol{x} \cdot \boldsymbol{y}}{\|\boldsymbol{x}\| \cdot \|\boldsymbol{y}\|}. \tag{13.2}$$

13.21. Poznámka. Zabývejme se otázkou, zda každé dva nenulové vektory mají definován úhel mezi sebou. Především podle poznámky ?? platí, že $\|\boldsymbol{x}\| \neq 0$, $\|\boldsymbol{y}\| \neq 0$, protože $\boldsymbol{x} \neq \boldsymbol{o}$, $\boldsymbol{y} \neq \boldsymbol{o}$. Takže se ve zlomku z rovnosti (13.2) nedělí nulou.

Aby existovalo φ takové, že platí (13.2), musí platit

$$-1 \leq \frac{\boldsymbol{x} \cdot \boldsymbol{y}}{\|\boldsymbol{x}\| \cdot \|\boldsymbol{y}\|} \leq 1.$$

Tento požadavek zaručuje následující věta.

13.22. Věta (Schwartzova nerovnost).* Nechť L je lineární prostor se skalárním součinem a $\boldsymbol{x} \in L$, $\boldsymbol{y} \in L$. Pak platí:

$$|\boldsymbol{x} \cdot \boldsymbol{y}| \leq \|\boldsymbol{x}\| \cdot \|\boldsymbol{y}\|. \tag{13.3}$$

Důkaz. Nechť $\alpha \in \mathbf{R}$. Násobme sám se sebou vektor $\boldsymbol{x} - \alpha\,\boldsymbol{y}$. Podle vlastnosti (4) definice ?? je

$$0 \leq (\boldsymbol{x} - \alpha\,\boldsymbol{y}) \cdot (\boldsymbol{x} - \alpha\,\boldsymbol{y}) = \boldsymbol{x} \cdot \boldsymbol{x} - \alpha \cdot 2(\boldsymbol{x} \cdot \boldsymbol{y}) + \alpha^2 \cdot (\boldsymbol{y} \cdot \boldsymbol{y}).$$

V úpravách jsme použili vlastnosti (2) a (3) definice ??. Označme $A = \boldsymbol{y} \cdot \boldsymbol{y} = \|\boldsymbol{y}\|^2$, $B = -2(\boldsymbol{x} \cdot \boldsymbol{y})$, $C = \boldsymbol{x} \cdot \boldsymbol{x} = \|\boldsymbol{x}\|^2$. Dostáváme

$$0 \leq A\,\alpha^2 + B\,\alpha + C.$$

Tato nerovnost musí platit pro všechna $\alpha \in \mathbf{R}$. Diskriminant této kvadratické nerovnice tedy nesmí být kladný. Z toho nám vyplývá podmínka pro čísla A, B, C:

$$B^2 - 4AC \leq 0, \quad \text{tj.} \quad B^2 \leq 4AC, \quad \text{tj.} \quad \big(-2(\boldsymbol{x} \cdot \boldsymbol{y})\big)^2 \leq 4\,\|\boldsymbol{x}\|^2\|\boldsymbol{y}\|^2,$$

$$\text{tj.} \quad (-2)^2\,(\boldsymbol{x} \cdot \boldsymbol{y})^2 \leq 4\,\|\boldsymbol{x}\|^2\|\boldsymbol{y}\|^2, \quad \text{tj.} \quad \sqrt{(\boldsymbol{x} \cdot \boldsymbol{y})^2} \leq \sqrt{\|\boldsymbol{x}\|^2}\sqrt{\|\boldsymbol{y}\|^2} \quad \text{tj.} \quad |\boldsymbol{x} \cdot \boldsymbol{y}| \leq \|\boldsymbol{x}\| \cdot \|\boldsymbol{y}\|.$$

13.23. Definice. Nechť L je lineární prostor se skalárním součinem. *Vzdálenost vektoru $\boldsymbol{x}$ od vektoru $\boldsymbol{y}$* definujeme jako $\|\boldsymbol{y} - \boldsymbol{x}\|$. Podle věty ?? je $\|\boldsymbol{y} - \boldsymbol{x}\| = \|\boldsymbol{x} - \boldsymbol{y}\|$, takže často mluvíme o *vzdálenosti dvou vektorů $\boldsymbol{x}$ a $\boldsymbol{y}$* (bez závislosti na jejich pořadí).

13.24. Věta (trojúhelníková nerovnost).* Pro velikosti vektorů platí

$$\|\boldsymbol{x}+\boldsymbol{y}\| \leq \|\boldsymbol{x}\| + \|\boldsymbol{y}\|. \tag{13.4}$$

Důkaz. $\|\boldsymbol{x}+\boldsymbol{y}\|^2 = (\boldsymbol{x}+\boldsymbol{y})\cdot(\boldsymbol{x}+\boldsymbol{y}) = \boldsymbol{x}\,\boldsymbol{x} + 2\,\boldsymbol{x}\,\boldsymbol{y} + \boldsymbol{y}\,\boldsymbol{y} \leq \|\boldsymbol{x}\|^2 + 2\,\|\boldsymbol{x}\|\cdot\|\boldsymbol{y}\| + \|\boldsymbol{y}\|^2 = \big(\|\boldsymbol{x}\| + \|\boldsymbol{y}\|\big)^2$. Ve výpočtu jsme použili Schwartzovu nerovnost ??. Po odmocnění dostáváme dokazovanou nerovnost.

13.25. Poznámka. Vysvětlíme si, proč se dokázaná nerovnost nazývá trojúhelníková. Tu někteří čtenáři znají geometricky formulovanou třeba takto: součet délek dvou stran v trojúhelníku je vždy větší než délka strany třetí. Nechť vektory $\boldsymbol{a}$, $\boldsymbol{b}$ a $\boldsymbol{c}$ jsou prvky lineárního prostoru se skalárním součinem a představme si je jako vrcholy pomyslného trojúhelníka. Velikost stran je totéž jako vzdálenost odpovídajících vektorů. Geometrické tvrzení o velikostech stran trojúhelníka tedy můžeme pomocí definice ?? přepsat takto:

$$\|\boldsymbol{a}-\boldsymbol{b}\| \leq \|\boldsymbol{a}-\boldsymbol{c}\| + \|\boldsymbol{c}-\boldsymbol{b}\|.$$

Při volbě $\boldsymbol{x} = \boldsymbol{a}-\boldsymbol{c}$, $\boldsymbol{y} = \boldsymbol{c}-\boldsymbol{b}$ přechází uvedená nerovnost na tvar (13.4).

13.26. Příklad. Uvažujme lineární prostor $\mathbf{R}^4$ se standardním skalárním součinem (13.1). Ukážeme, jak vypadá velikost vektoru $(1,2,3,4)$ a jaký je úhel mezi vektory $(1,2,3,4)$ a $(1,0,0,2)$.

Podle definice ?? a podle (13.1) je

$$\big\|(1,2,3,4)\big\| = \sqrt{(1,2,3,4)\cdot(1,2,3,4)} = \sqrt{1^2+2^2+3^2+4^2} = \sqrt{30}.$$

Podle definice ?? platí pro úhel φ následující rovnost:

$$\cos\varphi = \frac{(1,2,3,4)\cdot(1,0,0,2)}{\big\|(1,2,3,4)\big\|\cdot\big\|(1,0,0,2)\big\|} = \frac{1+0+0+4\cdot 2}{\sqrt{30}\cdot\sqrt{1+4}} = \frac{9}{\sqrt{150}}, \quad \text{tj.} \quad \varphi = \arccos\frac{9}{\sqrt{150}}.$$

13.27. Příklad. Označme symbolem U_O množinu orientovaných úseček v rovině se společným počátkem O. Ukážeme, že každá lineární transformace $\mathcal{A}\colon U_O \to U_O$ je rovna složení konečně mnoha otočení a změny měřítka.

Je-li hod $\mathcal{A} = 0$, pak transformace vše zobrazí do nulového vektoru. Takovou transformaci zapíšeme jako změnu měřítka s koeficienty $0, 0$.

Je-li hod $\mathcal{A} = 1$, pak transformace $\mathcal{A}$ je projekce. Jádrem zobrazení jsou vektory v jedné přímce. Aplikujme otočení, které zajistí, že tato přímka se kryje s první souřadnicovou osou. Pak aplikujeme změnu měřítka s koeficientem $0, r$ (jak zvolit parametr r je popsáno níže). Nakonec druhou souřadnicovou osu otočíme tak, aby se kryla s $\mathcal{A}(U_O)$.

Je-li hod $\mathcal{A} = 2$, pak dva na sebe kolmé bázové vektory s jednotkovou velikostí se zobrazí na dva lineárně nezávislé vektory $\boldsymbol{b}'_1, \boldsymbol{b}'_2$. Pokusíme se tyto vektory transformovat zpět pomocí otočení a změny měřítka na původní bázové vektory. Tím popíšeme $\mathcal{A}^{-1}$. Protože inverze k

otočení je otočení a inverze ke změně měřítka s nenulovými koeficienty je změna měřítka, je možné zapsat jako složení těchto transformací i původní transformaci $\mathcal{A}$.

Nejprve aplikujeme otočení, které způsobí, že delší z vektorů $\boldsymbol{b}'_1, \boldsymbol{b}'_2$ se kryje s první souřadicovou osou. Pak aplikujeme změnu měřítka s koeficienty $1, t$, která nemění delší z vektorů. Parametr t volíme tak, aby po změně měřítka měl (původně) kratší vektor stejnou velikost, jako jeho delší bráška. Dále provedeme otočení tak, aby osa úhlu těchto vektorů se kryla s první osou. Poté provedeme změnu měřítka s parametry $u, 1$, aby sledované vektory byly na sebe kolmé. Dále otočíme tyto vektory tak, aby se kryly s osami a nakonec provedeme změnu měřítka tak, aby měly jednotkovou velikost.

Jak zvolíme parametr r? Zvolme vektor $\boldsymbol{w}$, který leží v $\mathcal{A}(U_O)$ a má jednotkovou velikost. Jeho obraz $\mathcal{A}(\boldsymbol{w})$ také leží na přímce $\mathcal{A}(U_O)$, takže platí $\mathcal{A}(\boldsymbol{w}) = r\,\boldsymbol{w}$. Parametr r je tedy velikost obrazu $\mathcal{A}(\boldsymbol{w})$.

Jak zvolíme paramter t? Nechť delší vektor má velikost v a kratší vektor má souřadnice (a, b) vzhledem k bázi (B). Po změně měřítka má tento vektor souřadnice (a, tb) a má tedy velikost $\sqrt{a^2 + t^2b^2}$, což se musí rovnat v. Takže

$$a^2 + t^2b^2 = v^2, \qquad t^2b^2 = v^2 - a^2, \quad t = \sqrt{\frac{v^2 - a^2}{b^2}}.$$

Číslo $v^2 - a^2$ je zaručeně nezáporné, protože v^2 je větší než $a^2 + b^2$. Číslo b je nenulové, protože vektory jsou lineárně nezávislé.

Jak zvolíme parametr u? Nechť $\boldsymbol{b}_1''$ má souřadnice (a, b) vzhledem k bázi (B) a vektor $\boldsymbol{b}_2''$ má souřadnice $(a, -b)$ vzhledem ke stejné bázi. Po změně měřítka s parametry $u, 1$ budou mít tyto vektory souřadnice (ua, b), $(ua, -b)$. Mají být na sebe kolmé, tedy skalární součin těchto vektorů má být nulový:

$$(ua, b) \cdot (ua, -b) = u^2a^2 - b^2 = 0, \quad \text{takže} \quad u^2a^2 = b^2, \quad u = \frac{b}{a}.$$

13.28. Příklad. Nechť L je lineární prostor spojitých funkcí definovaných na konečném uzavřeném intervalu $D \subseteq \mathbf{R}$. Ukážeme, že předpis

$$f \cdot g = \int_D f(x)\, g(x)\, \mathrm{d}x$$

definuje skalární součin na lineárním prostoru L. Ověříme vlastnosti (1) až (4). Nechť $f \in L$, $g \in L$, $h \in L$ a $\alpha \in \mathbf{R}$. Pak platí

$$(1) \quad f \cdot g = \int_D f(x)\, g(x)\, \mathrm{d}x = \int_D g(x)\, f(x)\, \mathrm{d}x = g \cdot f,$$

$$(2) \quad (f+g) \cdot h = \int_D \big(f(x) + g(x)\big)\, h(x)\, \mathrm{d}x = \int_D \big(f(x)\, h(x) + g(x)\, h(x)\big)\, \mathrm{d}x =$$

$$= \int_D f(x)\, h(x)\, \mathrm{d}x + \int_D g(x)\, h(x)\, \mathrm{d}x = f \cdot h + g \cdot h,$$

$$(3) \quad (\alpha f) \cdot g = \int_D \alpha f(x)\, g(x)\, \mathrm{d}x = \alpha \cdot \int_D f(x)\, g(x)\, \mathrm{d}x = \alpha\, (f \cdot g),$$

$$(4) \quad f \cdot f = \int_D f^2(x)\, \mathrm{d}x \geq 0,$$

$$\int_D f^2(x)\, \mathrm{d}x = 0 \quad \text{jen tehdy, když } f(x) = 0\ \forall x \in D, \text{ protože } f \text{ je spojitá.}$$

Příklad ilustruje, že i na lineárních prostorech nekonečné dimenze jsme schopni definovat skalární součin. Z tohoto skalárního součinu odvozená *norma funkce f* $\|f\|$, „úhel φ mezi

funkcemi f a g“ a „vzdálenost dvou funkcí f a g“ $\|f-g\|$ se počítá takto:

$$\|f\| = \sqrt{\int_D f^2(x)\,\mathrm{d}x}, \quad \varphi = \arccos \frac{\int_D f(x)g(x)\,\mathrm{d}x}{\sqrt{\int_D f^2(x)\,\mathrm{d}x \int_D g^2(x)\,\mathrm{d}x}}, \quad \|f-g\| = \sqrt{\int_D \big(f(x)-g(x)\big)^2}$$

13.29. Poznámka. Protože máme na lineárních prostorech se skalárním součinem definován úhel mezi nenulovými vektory, můžeme pro každé dva nenulové vektory rozhodnout, kdy jsou na sebe kolmé. Je to tehdy, když je $\cos\varphi = 0$, neboli $\boldsymbol{x}\cdot\boldsymbol{y} = 0$. Z toho vyplývá následující definice.

13.30. Definice. Nechť L je lineární prostor se skalárním součinem. Dva nenulové vektory $\boldsymbol{x} \in L$ a $\boldsymbol{y} \in L$ *jsou na sebe kolmé* (značíme $\boldsymbol{x} \perp \boldsymbol{y}$), pokud je $\boldsymbol{x}\cdot\boldsymbol{y} = 0$.

13.31. Příklad. (Pythagorova věta.) Nechť $\boldsymbol{x} \in L$, $\boldsymbol{y} \in L$ jsou nenulové vektory, které jsou na sebe kolmé. Pak platí

$$\|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2 = \|\boldsymbol{x}-\boldsymbol{y}\|^2.$$

Zdůvodnění je jednoduché: $\|\boldsymbol{x}-\boldsymbol{y}\|^2 = (\boldsymbol{x}-\boldsymbol{y})\cdot(\boldsymbol{x}-\boldsymbol{y}) = \boldsymbol{x}\cdot\boldsymbol{x}-2\boldsymbol{x}\cdot\boldsymbol{y}+\boldsymbol{y}\cdot\boldsymbol{y} = \|\boldsymbol{x}\|^2-2\cdot 0+\|\boldsymbol{y}\|^2$. Geometrická interpretace tohoto příkladu je následující. Trojúhleník s vrcholy $\boldsymbol{o}$, $\boldsymbol{x}$ a $\boldsymbol{y}$ je pravoúhlý s pravým úhlem při vrcholu $\boldsymbol{o}$. Čísla $\|\boldsymbol{x}\|$, $\|\boldsymbol{y}\|$ jsou velikosti odvěsen a $\|\boldsymbol{x}-\boldsymbol{y}\|$ je velikost přepony.

13.32. Definice.* Nechť $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ je báze lineárního prostoru se skalárním součinem. Bázi B nazýváme *ortogonální*, pokud $\boldsymbol{b}_i \perp \boldsymbol{b}_j$ $\forall i \in \{1, 2, \ldots, n\}$, $\forall j \in \{1, 2, \ldots, n\}$, $i \neq j$.

Bázi B nazýváme *ortonormální*, pokud je ortogonální, a navíc $\|\boldsymbol{b}_i\| = 1, \forall i \in \{1, 2, \ldots, n\}$.

13.33. Věta. Báze $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ je ortonormální právě tehdy, když

$$\boldsymbol{b}_i \cdot \boldsymbol{b}_j = \begin{cases} 0 \text{ pro } i \neq j, \\ 1 \text{ pro } i = j. \end{cases}$$

Důkaz. Báze B je ortonormální právě tehdy, když (podle definice ??) platí $\boldsymbol{b}_i \cdot \boldsymbol{b}_j = 1$ pro $i = j$ a navíc je ortogonální, tj. $\boldsymbol{b}_i \perp \boldsymbol{b}_j$ pro $i \neq j$. To podle definice ?? znamená, že $\boldsymbol{b}_i \cdot \boldsymbol{b}_j = 0$ pro $i \neq j$.

13.34. Věta.* Nechť (B) je ortonormální uspořádaná báze lineárního prostoru L se skalárním součinem. Pak pro všechna $\boldsymbol{x} \in L$, $\boldsymbol{y} \in L$, $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)_{(B)}$, $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)_{(B)}$ lze skalární součin počítat ze souřadnic vektorů takto:

$$\boldsymbol{x} \cdot \boldsymbol{y} = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n.$$

Důkaz. Podle předpokladu je $\boldsymbol{x} = x_1\,\boldsymbol{b}_1 + x_2\,\boldsymbol{b}_2 + \cdots + x_n\,\boldsymbol{b}_n$, $\boldsymbol{y} = y_1\,\boldsymbol{b}_1 + y_2\,\boldsymbol{b}_2 + \cdots + y_n\,\boldsymbol{b}_n$. Počítejme $\boldsymbol{x} \cdot \boldsymbol{y}$:

$$\boldsymbol{x} \cdot \boldsymbol{y} = (x_1\,\boldsymbol{b}_1 + x_2\,\boldsymbol{b}_2 + \cdots + x_n\,\boldsymbol{b}_n) \cdot (y_1\,\boldsymbol{b}_1 + y_2\,\boldsymbol{b}_2 + \cdots + y_n\,\boldsymbol{b}_n) =$$

$$= x_1y_1\,\boldsymbol{b}_1\cdot\boldsymbol{b}_1 + x_1y_2\,\boldsymbol{b}_1\cdot\boldsymbol{b}_2 + \cdots + x_1y_n\,\boldsymbol{b}_1\cdot\boldsymbol{b}_n + x_2y_1\,\boldsymbol{b}_2\cdot\boldsymbol{b}_1 + x_2y_2\,\boldsymbol{b}_2\cdot\boldsymbol{b}_2 + \cdots + x_2y_n\,\boldsymbol{b}_2\cdot\boldsymbol{b}_n + \cdots + x_ny_n\,\boldsymbol{b}_n$$

$$= x_1y_1\cdot 1 + x_1y_2\cdot 0 + \cdots + x_1y_n\cdot 0 + x_2y_1\cdot 0 + x_2y_2\cdot 1 + \cdots + x_2y_n\cdot 0 + \cdots + x_ny_n\cdot 1 = x_1y_1 + x_2y_2 + \cdots + x_ny$$

V úpravách jsme využili větu ?? a toho, že báze B je ortonormální.

13.35. Příklad. Nechť $\mathbf{R}^n$ je lineární prostor se standardním skalárním součinem zavedeným v příkladu ??. Pak standardní báze

$$S = \big\{(1,0,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,0,0,\ldots,1)\big\}$$

je ortonormální bází.

13.36. Věta.* Nechť $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou nenulové vektory lineárního prostoru se skalárním součinem, které jsou na sebe navzájem kolmé, tj. $\boldsymbol{x}_i \cdot \boldsymbol{x}_j = 0$ pro $i \neq j$ a $\boldsymbol{x}_i \cdot \boldsymbol{x}_i > 0$. Pak jsou tyto vektory lineárně nezávislé.

Důkaz. Podle definice lineární nezávislosti stačí ověřit, že z rovnosti

$$\alpha_1 \cdot \boldsymbol{x}_1 + \alpha_2 \cdot \boldsymbol{x}_2 + \cdots + \alpha_n \cdot \boldsymbol{x}_n = \boldsymbol{o}$$

nutně plyne, že všechna čísla čísla α_i jsou nulová. Vynásobíme-li obě strany uvedené rovnosti skalárně vektorem $\boldsymbol{x}_i$, dostáváme na levé straně součet nul s výjimkou jediného sčítance, protože vektor $\boldsymbol{x}_i$ je kolmý na všechny všechny ostatní vektory $\boldsymbol{x}_j$. Máme tedy

$$\alpha_i \, \boldsymbol{x}_i \cdot \boldsymbol{x}_i = \boldsymbol{o} \cdot \boldsymbol{x}_i = 0.$$

Protože $\boldsymbol{x}_i \cdot \boldsymbol{x}_i$ je nenulové číslo, musí být $\alpha_i = 0$. Tuto operaci můžeme provést pro každý index $i \in \{1, 2, \ldots, n\}$, takže všechna čísla čísla α_i jsou nutně nulová.

13.37. Věta.* Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je ortonormální báze lineárního prostoru se skalárním součinem. Pak pro souřadnice libovolného vektoru $\boldsymbol{x}$ platí

$$\boldsymbol{x} = (\boldsymbol{x}\cdot\boldsymbol{b}_1,\ \boldsymbol{x}\cdot\boldsymbol{b}_2,\ \ldots,\ \boldsymbol{x}\cdot\boldsymbol{b}_n)_{(B)}.$$

Důkaz. Označme $\boldsymbol{y} = (\boldsymbol{x} \cdot \boldsymbol{b}_1)\, \boldsymbol{b}_1 + (\boldsymbol{x} \cdot \boldsymbol{b}_2)\, \boldsymbol{b}_2 + \cdots + (\boldsymbol{x} \cdot \boldsymbol{b}_n)\, \boldsymbol{b}_n$. Podle definice souřadnic vzhledem k bázi máme dokázat, že $\boldsymbol{x} = \boldsymbol{y}$. Násobme vektor $\boldsymbol{y}$ vektorem $\boldsymbol{b}_i$:

$$\boldsymbol{y} \cdot \boldsymbol{b}_i = \big((\boldsymbol{x} \cdot \boldsymbol{b}_1)\, \boldsymbol{b}_1 + (\boldsymbol{x} \cdot \boldsymbol{b}_2)\, \boldsymbol{b}_2 + \cdots + (\boldsymbol{x} \cdot \boldsymbol{b}_n)\, \boldsymbol{b}_n\big) \cdot \boldsymbol{b}_i = (\boldsymbol{x} \cdot \boldsymbol{b}_i)\, \boldsymbol{b}_i \cdot \boldsymbol{b}_i = \boldsymbol{x} \cdot \boldsymbol{b}_i,$$

protože báze (B) je ortonormální. Máme tedy výsledek $\boldsymbol{x} \cdot \boldsymbol{b}_i = \boldsymbol{y} \cdot \boldsymbol{b}_i \ \forall i \in \{1, 2, \ldots, n\}$.

Vektor $\boldsymbol{x} - \boldsymbol{y}$ je kolmý na všechny prvky $\boldsymbol{b}_i$, protože z předchozího výpočtu plyne $(\boldsymbol{x} - \boldsymbol{y}) \cdot \boldsymbol{b}_i = 0$. Pokud by $\boldsymbol{x} \neq \boldsymbol{y}$, pak podle věty ?? jsou vektory $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n, \boldsymbol{x} - \boldsymbol{y}$ lineárně nezávislé, ale to je ve sporu s tím, že (B) je báze. Musí tedy být $\boldsymbol{x} = \boldsymbol{y}$.

13.38. Poznámka. Předchozí věta má názornou geometrickou interpretaci. Souřadnice $\boldsymbol{x} \cdot \boldsymbol{b}_i$ jsou vlastně kolmé průměty vektoru $\boldsymbol{x}$ na vektory báze $\boldsymbol{b}_i$. O těchto pojmech pohovoříme podrobněji v následující kapitole.

13.39. Věta. Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je ortonormální báze lineárního prostoru se skalárním součinem a $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)_{(B)}$ je jeho libovolný vektor. Pak úhel φ_i mezi vektorem $\boldsymbol{x}$ a vektorem $\boldsymbol{b}_i$ lze počítat podle vzorce

$$\cos \varphi_i = \frac{x_i}{\|\boldsymbol{x}\|} .$$

Důkaz. Podle definice ?? je

$$\cos \varphi_i = \frac{\boldsymbol{x} \cdot \boldsymbol{b}_i}{\|\boldsymbol{x}\| \, \|\boldsymbol{b}_i\|} = \frac{\boldsymbol{x} \cdot \boldsymbol{b}_i}{\|\boldsymbol{x}\|} = \frac{x_i}{\|\boldsymbol{x}\|} .$$

V úpravách jsme využili toho, že $\|\boldsymbol{b}_i\| = 1$ (báze je ortonormální) a dále věty ??, podle které je $x_i = \boldsymbol{x} \cdot \boldsymbol{b}_i$.

13.40. Poznámka. Protože je $\|\boldsymbol{x}\|^2 / \|\boldsymbol{x}\|^2 = 1$ a dále je $\|\boldsymbol{x}\|^2 = x_1^2 + x_2^2 + \cdots + x_n^2$, plyne z věty ?? zajímavý důsledek:

$$\cos^2 \varphi_1 + \cos^2 \varphi_2 + \cdots + \cos^2 \varphi_n = 1,$$

kde φ_i jsou úhly mezi vektorem $\boldsymbol{x}$ a vektory ortonormální báze.

13.41. Poznámka. Je přirozené se ptát, zda každý lineární prostor (aspoň konečné dimenze) má ortonormální bázi. Věta ?? ukazuje, že každý lineární prostor má bázi. Následující věta ukazuje, že každá konečná báze se dá v jistém smyslu pozměnit tak, aby se z ní stala ortonormální báze.

13.42. Věta (Schmidtův ortogonalizační proces).* Nechť $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ je báze lineárního prostoru L se skalárním součinem. Pak existuje ortonormální báze $\{\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n\}$ taková, že

$$\langle \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k \rangle = \langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k \rangle, \qquad \forall k \in \{1, 2, \ldots, n\}.$$

Důkaz. Nejprve vysvětlíme ideu důkazu, která je v tomto případě asi důležitější než podrobné počítání. Vektor $\boldsymbol{c}_1$ volíme stejný jako $\boldsymbol{b}_1$ jen s tím rozdílem, že jej „normalizujeme“. To znamená, že jej násobíme vhodnou konstantou, aby $\|\boldsymbol{c}_1\| = 1$.

Představme si dále, že už jsme našli $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$ takové, že $\langle \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k \rangle = \langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$ a přitom vektory $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$ jsou na sebe vzájemně kolmé a mají jednotkovou velikost. Vektor $\boldsymbol{b}_{k+1}$ nyní „ortogonalizujeme“, tj. upravíme tak, aby byl kolmý na všechny vektory z $\langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k \rangle$. Ukážeme později, že k tomu účelu stačí od vektoru $\boldsymbol{b}_{k+1}$ odečíst určitou lineární kombinaci vektorů $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$. Takto upravený vektor dále „normalizujeme“, tj. vynásobíme vhodnou konstantou, aby $\|\boldsymbol{c}_{k+1}\| = 1$. Tím se jeho kolmost vůči ostatním vektorům z $\langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k \rangle$ nepokazí. Protože vektor $\boldsymbol{c}_{k+1}$ vznikl jako lineární kombinace vektorů

$\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k, \boldsymbol{b}_{k+1}$, je

$$\langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k, \boldsymbol{c}_{k+1} \rangle = \langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k, \boldsymbol{b}_{k+1} \rangle = \langle \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_{k+1} \rangle.$$

Tím jsme rozšířili naši novou postupně budovanou ortonormální bázi o další vektor. Opakovaným použitím tohoto postupu dostáváme hledanou ortonormální bázi $\{\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n\}$.

Nyní stačí jen podrobněji ukázat, jak se vektor „normalizuje“ a „ortogonalizuje“. Normalizaci libovolného vektoru $\boldsymbol{x}$ provedeme tak, že položíme $\boldsymbol{x}' = (1/\|\boldsymbol{x}\|) \cdot \boldsymbol{x}$. Skutečně je:

$$\|\boldsymbol{x}'\|^2 = \boldsymbol{x}' \cdot \boldsymbol{x}' = \frac{1}{\|\boldsymbol{x}\|}\,\boldsymbol{x} \cdot \frac{1}{\|\boldsymbol{x}\|}\,\boldsymbol{x} = \frac{1}{\|\boldsymbol{x}\|^2}\,\boldsymbol{x}\,\boldsymbol{x} = \frac{1}{\|\boldsymbol{x}\|^2}\,\|\boldsymbol{x}\|^2 = 1.$$

Nechť $\boldsymbol{b}_{k+1} \notin \langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k \rangle$ a nechť vektory $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$ jsou na sebe navzájem kolmé a mají jednotkovou velikost. Vektor $\boldsymbol{b}_{k+1}$ „ortogonalizujeme“ tak, že položíme

$$\boldsymbol{b}'_{k+1} = \boldsymbol{b}_{k+1} - \sum_{i=1}^{k} (\boldsymbol{b}_{k+1} \cdot \boldsymbol{c}_i)\,\boldsymbol{c}_i.$$

Nově vytvořený vektor $\boldsymbol{b}'_{k+1}$ je kolmý na všechny vektory $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$, protože:

$$\boldsymbol{b}'_{k+1} \cdot \boldsymbol{c}_j = \left(\boldsymbol{b}_{k+1} - \sum_{i=1}^{k} (\boldsymbol{b}_{k+1} \cdot \boldsymbol{c}_i)\,\boldsymbol{c}_i \right) \cdot \boldsymbol{c}_j = \boldsymbol{b}_{k+1} \cdot \boldsymbol{c}_j - \sum_{i=1}^{k} (\boldsymbol{b}_{k+1} \cdot \boldsymbol{c}_i)\,(\boldsymbol{c}_i \cdot \boldsymbol{c}_j) = \boldsymbol{b}_{k+1} \cdot \boldsymbol{c}_j - \boldsymbol{b}_{k+1} \cdot \boldsymbol{c}_j = 0$$

V uvedeném součtu jsou ostatní sčítanci nuloví, protože vektory $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$ jsou podle předpokladu na sebe navzájem kolmé.

13.43. Definice. Matice $\mathbf{A} \in \mathbf{R}^{n,n}$, pro kterou platí $\mathbf{A}^T \cdot \mathbf{A} = \mathbf{E}$, se nazývá *ortogonální*.

13.44. Věta. Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$. V $\mathbf{R}^n$ předpokládejme standardní skalární součin. Následující podmínky jsou ekvivalentní:

(1) $\mathbf{A}$ je ortogonální.
(2) $\mathbf{A} \cdot \mathbf{A}^T = \mathbf{E}$
(3) $\mathbf{A}^T$ je ortogonální
(4) $\mathbf{A}$ obsahuje ve sloupcích ortonormální bázi $\mathbf{R}^n$.
(5) $\mathbf{A}$ obsahuje v řádcích ortonormální bázi $\mathbf{R}^n$.
(6) $\mathbf{A}$ je maticí přechodu mezi dvěma ortonormálními bázemi.
(7) $\mathbf{A}$ je maticí transformace, kterí zobrazí ortonormální bázi na ortonormální bázi.

Důkaz. (1)⇒(2): Protože $\mathbf{A}^T \cdot \mathbf{A} = \mathbf{E}$, je $\mathbf{A}$ regulární a $\mathbf{A}^{-1} = \mathbf{A}^T$. Inverzní matice k matici $\mathbf{A}$ vždy komutuje s maticí $\mathbf{A}$.

(2)⇒(3): Přímo z definice ortogonální matice.

(3)⇒(1): Protože $(\mathbf{A}^T)^T = \mathbf{A}$.

(1)⇔(4): Rovnost $\mathbf{A}^T \cdot \mathbf{A}$ rozepsaná po sloupcích matice $\mathbf{A} = (\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n)$ říká, že $\boldsymbol{a}_i^T \cdot \boldsymbol{a}_j = 0$ pro $i \neq j$ a $\boldsymbol{a}_i^T \cdot \boldsymbol{a}_i = 1$. Přitom součin $\boldsymbol{a}_i^T \cdot \boldsymbol{a}_j$ je standarní skalární součin v $\mathbf{R}^n$.

(4)⇔(5): protože (1)⇔(3).

(4)⇒(6): $\mathbf{A}$ je maticí přechodu od strandardní báze k bázi $\mathbf{A} = (\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n)$, kterí je podle předpokladu ortogonální.

(6)⇒(1): $\mathbf{A} = (\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n)$. Sloupce $\boldsymbol{a}_i$ obsahují podle ?? souřadnice vektorů $\boldsymbol{b}_i$ vzhledem k ortogonální bázi (C), přitom $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je také ortonormální báze. Takže $\boldsymbol{b}_i \cdot \boldsymbol{b}_j$ je rovno nule pro $i \neq j$ a jedné pro $i = j$. Podle věty ?? se skalární součin vektorů $\boldsymbol{b}_i$ dají spočítat pomocí souřadnic: $\boldsymbol{a}_i^T \cdot \boldsymbol{a}_j = 0$ pro $i \neq j$ a $\boldsymbol{a}_i^T \cdot \boldsymbol{a}_i = 1$, takže $\mathbf{A}$ je ortogonální.

(6)⇔(7): Viz definici matice přechodu ??.

13.45. Příklad. Matice otočení a matice osové souměrosti jsou ortogonální:

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Skutečně:

$$\begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Tyto matice jsou maticemi transformací, které zobrazují ortonormální bázi na ortonormální bázi (transformace zachovává velikosti a úhly).

13.46. Věta. (1) Je-li $\mathbf{A}$ ortogonální, pak $\det \mathbf{A} = 1$ nebo $\det \mathbf{A} = -1$.

(2) Součin ortogonálních matice je ortogonální.

(3) Je-li $\mathbf{A}$ ortogonální a je-li $\mathbf{x}$ sloupcový vektor, pak $\mathbf{A}\cdot\mathbf{x}$ má stejnou velikost jako vektor $\mathbf{x}$.

Důkaz. (1): $1 = \det \mathbf{E} = \det(\mathbf{A}\cdot\mathbf{A}^T) = (\det \mathbf{A})\,(\det \mathbf{A}^T) = (\det \mathbf{A})^2$.
(2): $(\mathbf{A}\cdot\mathbf{B})^T\cdot(\mathbf{A}\cdot\mathbf{B}) = \mathbf{B}^T\cdot\mathbf{A}^T\cdot\mathbf{A}\cdot\mathbf{B} = \mathbf{B}^T\cdot\mathbf{E}\cdot\mathbf{B} = \mathbf{E}$.
(3): $\|\mathbf{A}\mathbf{x}\|^2 = (\mathbf{A}\mathbf{x})^T\cdot(\mathbf{A}\mathbf{x}) = \mathbf{x}^T\cdot\mathbf{A}^T\cdot\mathbf{A}\cdot\mathbf{x} = \mathbf{x}^T\cdot\mathbf{x} = \|\mathbf{x}\|^2$.

13.47. Věta. Je-li $\mathbf{A}$ regulární matice, pak existuje ortogonální matice $\mathbf{Q}$ a horní trojúhelníková matice $\mathbf{R}$ tak, že

$$\mathbf{A} = \mathbf{Q}\cdot\mathbf{R}.$$

Důkaz. Sloupce matice $\mathbf{A}$ tvoří nějakou bázi (B). Tuto bázi pozměníme Schmidtovým ortogonalizačním procesem ?? na ortonormální bázi (C). Bázi (C) zapíšeme do sloupců matice $\mathbf{Q}$. Matice $\mathbf{R}$ je maticí přechodu od ortonormální báze (C) k bázi (B). Obsahuje souřadnice vektorů $\boldsymbol{b}_k$ z báze (B) vzhledem k (C). Díky vlastnosti Schmidtova ortogonalizačního procesu

$$\langle \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k\rangle = \langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k\rangle, \qquad \forall k \in \{1, 2, \ldots, n\}.$$

jsou souřadnice vektoru $\boldsymbol{b}_k$ vzhledem k (C) pro $i > k$ nulové, takže $\mathbf{R}$ je horní trojúhelníková.

13.48. Poznámka. Ortogonální matice jsou hojně používány v numerických metodách, neboť jsou numericky stabilní. Díky (3) věty ?? se totiž násobením ortogonální maticí chyba nezvětšuje.

Věta o QR rozkladu je jen jiný pohled na Schmidtův ortogonalizační proces. Říká, že máme-li ve sloupcích matice $\mathbf{A}$ nějakou bázi, pak ji můžeme „narovnat“, aby byla ortonormální a takto opravenou bázi zapsat do matice $\mathbf{Q}$. Přitom matice $\mathbf{R}$ je maticí koeficientů tohoto „narovnání“.

Dá se ukázat, že ortonogonální matice je vždy maticí nějakého otočení (při větší dimenzi je možné otáčet v různých směrech). Toto otočení je případně složeno s osovou souměrností (ve více dimenzích překlopením jednoho bázového vektoru do „protisměru“).

V případě matic $\mathbf{A} \in \mathbf{C}^{n,n}$ je analogií ortogonální matice tzv. *unitární matice* definovaná v ??. Důvod použití komplexně sdružených čísel v definici unitární matice souvisí s axiomem (1) skalárního součinu ??, který je pro komplexní čísla modifikován v souladu s poznámkou ??.

13.49. Definice. Matice $\mathbf{A}^H \in \mathbf{C}^{n,m}$ se nazývá *Hermitovsky sdružená* k matici $\mathbf{A} \in \mathbf{C}^{m,n}$ pokud je transponovaná a místo každého prvku je v matici zapsán prvek komplexně sdružený.

Matice $\mathbf{A} \in \mathbf{C}^{n,n}$ se nazývá *unitární*, pokud $\mathbf{A}^H \cdot \mathbf{A} = \mathbf{E}$.

13.50. Shrnutí. V lineárním prostoru jsme zavedli skalární součin pomocí axiomů /??/. Ukázali jsme, že axiomy vyhovují nejen standardnímu skalárnímu součinu /??/, ale je možné zavést i jiné skalární součiny.

Je-li na lineárním prostoru L definován skalární součin, pak je možno měřit velikosti vektorů /??/ a úhly mezi nenulovými vektory /??/. Abychom měli jistotu, že vzorec pro úhel dává výsledek pro libovolné nenulové vektory, museli jsme dokázat Schwartzovu nerovnost /??/.

Dva nenulové vektory jsou na sebe kolmé, právě když jejich skalární součin je roven nule. Zavedli jsme ortonormální bázi /??/ a ukázali důležité vlastnosti této báze /??, ??, ??/.

Ukázali jsme, že lze každou konečnou bázi upravit Schmidtovým ortogonalizačním procesem tak, aby upravená báze byla ortonormální, přitom lineární obaly prvních k vektorů obou bází zůstávají shodné.

Základní vlastnosti ortogonální matice /??/ jsou shrnuty v ??, ?? a ??.

14. Polynomy

14.1. Poznámka. S polynomy jsme se v tomto textu už na mnoha místech setkali. Pracovali jsme s nimi jako s funkcemi danými jistým vzorcem a shledali jsme, že množina polynomů tvoří lineární prostor. V této kapitole se na polynomy podíváme poněkud důkladněji a budeme vyšetřovat zejména vlastnosti jejich kořenů.

14.2. Poznámka. Na polynom se můžeme dívat dvěma pohledy. Buď jako na funkci danou jistým vzorcem (definice ??) nebo polynom ztotožníme s tím vzorečkem samotným (definice ??). Každý přístup vede k jinému způsobu porovnávání dvou polynomů, sčítání polynomů a násobení polynomu konstantou nebo polynomem.

Zavedeme tedy lineární prostor polynomů jednak jako podprostor funkcí se sčítáním a násobením obvyklým pro funkce. Dále zavedeme jiný lineární prostor polynomů jako vzorečků se sčítáním a násobením těch vzorečků. Nakonec ukážeme, že tyto dva lineární prostory jsou izomorfní, tedy, že mezi polynomy jako funkcemi a polynomy jako vzorečky existuje vzájemně jednoznačný vztah.

Pokud se čtenář nechce zatěžovat intuitivně samozřejmými úvahami o tom, že polymom vnímaný jako vzoreček podle definice ?? je víceméně totéž, co polynom vnímaný jako funkce podle definice ??, může následující text přeskočit a pokračovat až definicí ??.

14.3. Definice. *Polynom* je reálná funkce reálné proměnné, tedy $p\colon \mathbf{R} \to \mathbf{R}$, která má pro všechna $x \in \mathbf{R}$ funkční hodnotu $p(x)$ danou vzorcem

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \tag{14.1}$$

kde $a_0, \ldots, a_n$ jsou nějaká reálná čísla, která nazýváme *koeficienty* polynomu. Jinými slovy: je-li funkce p polynomem, existuje přirozené číslo n a konstanty $a_0, \ldots, a_n$ tak, že pro funkční hodnoty $p(x)$ platí uvedený vzorec pro všechna $x \in \mathbf{R}$.

14.4. Poznámka. Dva polynomy p a q podle této definice se rovnají, pokud se rovnají jako funkce, tedy pokud $p(x) = q(x)$ pro všechna $x \in \mathbf{R}$. Součet dvou polynomů p a q je funkce $p + q$, pro kterou je $(p + q)(x) = p(x) + q(x)$ pro všechna $x \in \mathbf{R}$. Konečně pro $\alpha \in \mathbf{R}$ je α-násobek polynomu p taková funkce αp, pro kterou platí $(\alpha p)(x) = \alpha \cdot p(x)$ pro všechna $x \in \mathbf{R}$.

14.5. Příklad. Funkce, jejíž hodnota v bodě $x \in \mathbf{R}$ je daná vzorcem $x^3 - 2x^2 - 4$, je polynom. Jeho koeficienty jsou $a_0 = -4$, $a_1 = 0$, $a_2 = -2$ a $a_3 = 1$. Povšimněme si, že je zde použit vzorec (14.1) v opačném pořadí „od nejvyšší mocniny proměnné k mocninám nižším“. Toto je dost častý zápis vzorců pro polynomy. Vzhledem k tomu, že sčítání reálných čísel je komutativní, na pořadí sčítanců nezáleží.

14.6. Příklad. Funkce exp, jejíž hodnota v bodě $x \in \mathbf{R}$ je daná vzorcem $\exp(x) = e^x$, není polynom. To znamená, že neexistuje konečné množství konstant $a_0, a_1, \ldots, a_n$ takové, že e^x lze vypočítat podle vzorce (14.1) pro všechny $x \in \mathbf{R}$. Abychom to dokázali, vypůjčíme si znalosti z analýzy. Je zřejmé, že pokud opakovaně derivujeme vzorec (14.1) podle proměnné x více než n krát, dostáváme nulovou funkci. Takže každý polynom p má tu vlastnost, že pro něj existuje přirozené číslo k takové, že k-tá derivace polynomu p je nulová funkce. Je známo, že funkce exp je odolná vůči libovolnému množství derivování: dostáváme zase funkci exp, která je nenulová. Takže tato funkce nemůže být polynom. Z analogických důvodů například funkce sinus a kosinus nejsou polynomy. Poznamenejme ještě, že hodnoty uvedených funkcí se dají přibližně počítat pomocí polynomů (tzv. *Taylorovy polynomy*). Toto téma ovšem překračuje rámec tohoto textu.

14.7. Poznámka. Následuje alternativní definice polynomu, v algebře možná obvyklejší:

14.8. Definice. *Polynom* je vzoreček

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \tag{14.2}$$

kde $a_0, \ldots, a_n$ jsou nějaká reálná čísla, která nazýváme *koeficienty* polynomu a x je formální proměnná (která samozřejmě může být označena jiným písmenem).

Polynom v tomto pojetí je určen jednoznačně konečně mnoha koeficienty $a_0, \ldots, a_n$, pomocí kterých lze uvedený vzoreček sestavit.

Hodnota polynomu s koeficienty $a_0, \ldots, a_n$ v bodě α je číslo $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n$.

14.9. Definice. Předpokládejme definici polynomů ??. Nechť polynom p má koeficienty $a_0, \dots, a_m$ a polynom q má koeficienty $b_0, \dots, b_n$. Bez újmy na obecnosti předpokládejme, že $m \leq n$. Definujeme:

Rovnost polynomů: Říkáme, že $p = q$ (tj. polynomy se rovnají), pokud $a_i = b_i$ pro $i \in \{0, \dots, m\}$ a při $m < n$ je navíc $b_i = 0$ pro $i \in \{m+1, \dots, n\}$.

Součet polynomů: Polynom $p + q$ má koeficienty $a_0 + b_0, \dots, a_m + b_m, b_{m+1}, \dots, b_n$.

Násobek polynomu p číslem α je polynom s koeficienty $\alpha a_0, \alpha a_1, \dots, \alpha a_m$.

14.10. Poznámka. Tato definice vymezuje algoritmy, které poznají rovnost polynomů a provedou součet a α-násobek polynomu. Všimněte si, že těmto algoritmům stačí pracovat s polynomy jen pomocí jejich koeficientů. Nemusejí implementovat kompletně celý vzoreček (14.2).

14.11. Příklad. Dva polynomy $0x^3 + 0x^2 - 2x + 3$ a $-2x + 3$ se rovnají, ačkoli ten první má čtyři koeficienty a ten druhý jen dva. Koeficienty a_0 a a_1 mají ale oba polynomy stejné.

Součtem polynomů $x^3 + 3x^2 - 2x$ a $5x + 7$ je polynom $x^3 + 3x^2 + 3x + 7$, protože má následující koeficienty (po řadě od koeficientu s indexem nula): $0 + 7$, $-2 + 5$, 3, 1.

14.12. Věta. Množina vzorečků tvaru (14.2), ve které dva vzorečky považujeme za totožné podle pravidla v definici ?? a na které je definováno sčítání a násobení konstantou podle stejné definice ??, tvoří lineární prostor. Tuto množinu označíme symbolem $\mathcal{P}_X$.

Důkaz. Součet dvou prvků z $\mathcal{P}_X$ je prvek v $\mathcal{P}_X$, α-násobek prvku z $\mathcal{P}_X$ je prvek v $\mathcal{P}_X$. Dále je třeba ověřit platnost axiomů (1) až (7) z definice ??. To přenecháme pečlivému čtenáři.

14.13. Poznámka. Definice ?? rovnosti, součtu a násobku vychází přirozeně z toho, jak bychom porovnávali, sčítali a násobili vzorečky tvaru (14.2). Je to ovšem jiná definice, než vyplývá z poznámky ??. Určitou práci nám dá uvést oba tyto světy do souvislosti.

V definici ?? mluvíme o *hodnotě polynomu*. Tím je každému reálnému číslu α přiřazena funkční hodnota polynomu, tedy polynom daný vzorečkem se stává funkcí. To popisuje jednoznačný přechod od polynomu v podobě vzorečku k polynomu jako funkci. Ukazuje se, že obráceně (od funkce ke vzorečku) to je malinko složitější:

14.14. Věta. Každá funkce $p\colon \mathbf{R} \to \mathbf{R}$, která je polynomem podle definice ??, má své koeficienty určeny jednoznačně. Přesněji: pokud funkce p je polynomem jednak s koeficienty $a_0, \dots, a_m$ a také s koeficienty $b_0, \dots, b_n$, pak pro tyto koeficienty platí rovnost podle definice ??.

Důkaz. K důkazu věty potřebujeme nejprve ověřit následující tvrzení:

14.15. Věta. Nulová funkce $\mathbf{R} \to \mathbf{R}$ je polynom, který musí mít všechny koeficienty nulové.

Důkaz. Uvažujme nulovou funkci p, která je dána vzorcem (14.1). Máme dokázat, že všechny koeficienty $a_0, a_1, \dots, a_n$ jsou nulové. Především je $p(0) = a_0$ (stačí do vzorce dosadit $x = 0$).

Protože $p(0) = 0$, je nutně $a_0 = 0$. Hodnotu funkce p v bodě x můžeme tedy zapsat ve tvaru:

$$0 = p(x) = x\,(a_1 + a_2 x + \ldots + a_n x^{n-1}) = x \cdot q(x).$$

Polynom q musí mít nulové hodnoty pro všechna $x \neq 0$. Protože q je spojitá funkce, je také $q(0) = 0$. Po dosazení $x = 0$ do vzorce pro $q(x)$ dostáváme $a_1 = 0$. Nyní můžeme psát

$$0 = p(x) = x^2(a_2 + a_3 x + \ldots + a_n x^{n-1}) = x^2 \cdot q_2(x)$$

a úvahu můžeme zopakovat. Dostáváme $a_2 = 0$. Matematickou indukcí lze ukázat, že $a_k = 0$ pro všechna $k \in \{0, 1, \ldots, n\}$.

Pokračování důkazu věty ??. Nechť $p(x) = a_0 + a_1 x + \cdots + a_m x^m = b_0 + b_1 x + \cdots + b_n x^n$ pro všechna $x \in \mathbf{R}$. Bez újmy na obecnosti lze předpokládat $m \leq n$. Odečtením dostaneme

$$p(x) - p(x) = (b_0 - a_0) + (b_1 - a_1)\,x + \ldots + (b_m - a_m)\,x^m + b_{m+1}x^{m+1} + \ldots + b_n x^n \quad \forall x \in \mathbf{R},$$

což je nulová funkce. Podle věty ?? má tento nulový polynom všechny koeficienty nulové, tedy musí $a_k = b_k$ pro všechna $k \in \{0, 1, \ldots, m\}$ a musí $b_k = 0$ pro všechna $k \in \{m+1, \ldots, n\}$.

14.16. Věta. Zobrazení z lineárního prostoru $\mathcal{P}_X$ (viz větu ??) do lineárního prostoru funkcí, které vzorečku (14.2) přiřadí funkci $p\colon \mathbf{R} \to \mathbf{R}$ předpisem (14.1), je lineární.

Důkaz. Je třeba dokázat, že součtem polynomů p a q podle definice ?? dostáváme polynom $p+q$, pro který platí $(p+q)(x) = p(x)+q(x)$ pro všechna $x \in \mathbf{R}$. Nechť polynom p má koeficienty $a_0, \ldots, a_m$ a polynom q má koeficienty $b_0, \ldots, b_n$. Bez újmy na obecnosti lze předpokládat $m \leq n$. Je

$$\begin{aligned}(a_0 + a_1x + a_2x^2 + \cdots + a_mx^m) + (b_0 + b_1x + b_2x^2 + \cdots + b_nx^n) = \\ = (a_0 + b_0) + (a_1 + b_1)\,x + (a_2 + b_2)\,x^2 + \cdots + (a_m + b_m)\,x^m + b_{m+1}x^{m+1} + \ldots + b_nx^n,\end{aligned}$$

pro všechna $x \in \mathbf{R}$, takže požadovaná rovnost platí. Také je

$$\alpha\,(a_0 + a_1x + a_2x^2 + \cdots + a_mx^m) = \alpha\,a_0 + \alpha\,a_1x + \alpha\,a_2x^2 + \cdots + \alpha\,a_mx^m,$$

pro všechna $x \in \mathbf{R}$, jinými slovy $\alpha\,p(x) = (\alpha p)(x)$ pro všechna $x \in \mathbf{R}$. Zobrazení je tedy lineární.

14.17. Věta. Zobrazení z lineárního prostoru $\mathcal{P}_X$ (viz větu ??) do lineárního prostoru polynomů jako funkcí, které vzorečku přiřadí funkci předpisem (14.1), je izomorfismus.

Důkaz. Zmíněné zobrazení je prosté (věta ??), je na (protože každý polynom jako funkce má svůj vzoreček) a je lineární (věta ??).

14.18. Poznámka. Důsledkem této věty je tvrzení, že součet polynomů (jako funkce) je polynom a také α-násobek polynomu je polynom. Stačí od funkcí přejít pomocí inverzního izomorfismu ke vzorečkům, tam provést součet (nebo α-násobek) a výsledek přenést zpět do prostoru polynomů jako funkcí.

14.19. Definice. Nechť polynom p má koeficienty $a_0, a_1, \ldots, a_n$. *Stupeň polynomu* je největší index k takový, že $a_k \neq 0$. Má-li polynom všechny koeficienty nulové (tzv. *nulový polynom*), prohlásíme, že jeho stupeň je roven -1.

14.20. Příklad. Polynom $0x^5 + 0x^4 + 5x^3 - 4x^2 + 2x + 7$ má koeficienty $a_0 = 7$, $a_1 = 2$, $a_2 = -4$, $a_3 = 5$, $a_4 = 0$, $a_5 = 0$. Takže největší index nenulového koeficientu je 3. Polynom má stupeň tři.

14.21. Definice. *Součin polynomů* p a q je funkce u daná předpisem $u(x) = p(x)\,q(x)$ pro všechna $x \in \mathbf{R}$. Součin polynomů p a q značíme pq.

14.22. Věta. Nechť p má koeficienty $a_0, a_1, \ldots, a_m$ a q má koeeficienty $b_0, b_1, \ldots, b_n$. Pak součin polynomů pq je polynom s koeficienty c_k pro $k \in \{0, 1, \ldots, m+n\}$ takovými, že

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0,$$

přičemž v tomto vzorci klademe $a_i = 0$ pro $i > m$ a $b_i = 0$ pro $i > n$.

Důkaz. Je $p(x) = a_0 + a_1x + \cdots + a_mx^m$ a $q(x) = b_0 + b_1x + \cdots + b_nx^n$. Pro všechna $x \in \mathbf{R}$ spočítáme $p(x)\,q(x)$. Pro větší pohodlí přitom značíme $a_i = 0$ pro $i > m$ a $b_i = 0$ pro $i > n$.

$$p(x)\,q(x) = (a_0 + a_1x + \cdots + a_mx^m) \cdot (b_0 + b_1x + \cdots + b_n + x^n) = (a_0b_0) + (a_0b_1 + a_1b_0)\,x + \\ + (a_0b_2 + a_1b_1 + a_2b_0)\,x^2 + \cdots + (a_0b_{m+n} + a_1b_{m+n-1} + \cdots + a_{m+n}b_0)\,x^{m+n}.$$

14.23. Věta. Nechť p je polynom stupně m a q je polynom stupně n. Pak $p + q$ je polynom stupně nejvýše $\max(m, n)$, $\alpha\,p$ je polynom stupně m pro $\alpha \neq 0$ a je to polynom stupně -1 pro $\alpha = 0$. Konečně pro nenulové polynomy p a q je pq polynom stupně $m + n$. Je-li p nebo q nulový, pak pq je polynom stupně -1.

Důkaz. Tvrzení plyne přímo z vět o počítání koeficientů součtu a součinu polynomů a z definice stupně polynomu.

14.24. Poznámka. Je potřeba si uvědomit, že stupeň součtu polynomů nemusí dosahovat maximum stupňů jednotlivých polynomů, které sčítáme. Kupříkladu

$$(x^3 + 2x^2 - x + 1) + (-x^3 - 2x^2 + 2x + 3) = x + 4.$$

Součet těchto polynomů stupně 3 je polynom stupně 1. Je dobré si také uvědomit, že stupeň součtu určitě nabývá maxima stupňů jednotlivých polynomů, které sčítáme, pokud stupně sčítaných polynomů jsou různé.

14.25. Poznámka. Podíl dvou polynomů (definovaný jako podíl funkcí) nemusí být polynom. Nechť jsou dány polynomy p a q, přitom q je nenulový. Je možné provést aspoň částečný podíl těchto polynomů se zbytkem, tedy najít takové polynomy r a z, aby polynom z měl menší stupeň než q a aby platilo

$$\frac{p(x)}{q(x)} = r(x) + \frac{z(x)}{q(x)}$$

pro všechna $x \in \mathbf{R}$ taková, že $q(x) \neq 0$. V tomto kontextu říkáme polynomu r *částečný podíl* polynomů p a q. Polynomu z říkáme *zbytek* po dělení polynomu p polynomem q. Následující věta ukazuje, že pro každé polynomy p a q (q nenulový) existuje jejich částečný podíl a zbytek po jejich dělení. Přitom jsou polynomy r a z určeny jednoznačně.

14.26. Věta. Nechť p, q jsou polynomy, q nenulový. Pak existuje právě jeden polynom r a právě jeden polynom z tak, že (i) $p = rq + z$, (ii) stupeň z je menší než stupeň q.

Důkaz. Existence polynomů r a z vyplývá z následujícího algoritmu, pomocí kterého je možné tyto polynomy na základě daných polynomů p a q najít.

(1) Položme $r = 0$ (nulový polynom) a $z = p$. Dále označme písmenem n stupeň polynomu q a písmenem c jeho koeficient s indexem n (tj. nenulový koeficient u nejvyšší mocniny polynomu q).
(2) Je-li stupeň z menší než n, algoritmus končí.

(3) Nechť m je stupeň polynomu z a nechť d je jeho koeficient s indexem m (koeficient u nejvyšší mocniny). Platí $m \geq n$, protože není splněna podmínka z kroku (2). K polynomu r přičteme polynom daný vzorcem $(d/c)\, x^{m-n}$ a od polynomu z odečteme polynom daný vzorcem $(d/c)\, x^{m-n}\, q(x)$. Vznikají nové polynomy r_1 a z_1, které dále označíme r a z a vracíme se ke kroku (2).

V kroku (3) se snižuje stupeň polynomu z, protože se od tohoto polynomu odečítá sčítanec s nejvyšší mocninou. Tím je zaručeno, že stupeň polynomu z postupně klesá a algoritmus určitě skončí. Krok (2) navíc zaručuje, že je splněno (ii) z tvrzení věty. Další vlastností algoritmu je skutečnost, že v každém okamžiku platí pro polynomy r a z podmínka (i), takže tato podmínka je splněna i po ukončení algoritmu. Především v kroku (1) je $r = 0$ a $z = p$, takže $rq + z = 0q + p = p$ a podmínka (i) je splněna. Dále v kroku (3) máme zaručeno, že $p = rq + z$ a ukážeme, že platí také $p = r_1 q + z_1$. Pro všechna $x \in \mathbf{R}$ je

$$r_1(x)\, q(x) + z_1(x) = \left(r(x) + \frac{d}{c}\, x^{m-n}\right) q(x) + \left(z(x) - \frac{d}{c}\, x^{m-n}\, q(x)\right) =$$

$$= r(x)\, q(x) + \frac{d}{c}\, x^{m-n}\, q(x) + z(x) - \frac{d}{c}\, x^{m-n}\, q(x) = r(x)\, q(x) + z(x) = p(x).$$

Jednoznačnost polynomů r a z je jednoduchým důsledkem věty o stupni součtu a součinu polynomů. Kdyby existovaly polynomy r_2 a z_2, které rovněž splňují (i) a (ii), pak je $p = rq + z = r_2 q + z_2$, takže $(r - r_2)\, q = z_2 - z$. Kdyby $r - r_2$ nebyl nulový polynom, pak stupeň

polynomu $(r-r_2)q$ by byl větší nebo roven stupni q, zatímco polynom z_2-z má stupeň menší než q. To je ovšem spor. Takže musí $r-r_2$ být nulový polynom a pak nutně též z_2-z je nulový polynom. Jinými slovy $r=r_2$ a $z=z_2$, takže polynomy r, z jsou určeny podmínkami (i) a (ii) jednoznačně.

14.27. Příklad. Najdeme částečný podíl a zbytek při dělení polynomu $2x^5-3x^4+3x^3-x^2-6x+8$ polynomem x^2-2x+4.

Algoritmus popsaný v důkazu věty ?? se zapisuje většinou do následujícího schématu:

$$
\begin{array}{r}
(2x^5-3x^4+3x^3-\ x^2-\ 6x+\ 8)\ :\ (x^2-2x+4)=2x^3+x^2-3x-11\\
-(2x^5-4x^4+8x^3)\\
\hline
x^4-5x^3-\ x^2-\ 6x+\ 8\\
-(x^4-2x^3+4x^2)\\
\hline
-3x^3-5x^2-\ 6x+\ 8\\
-(-3x^3+6x^2-12x)\\
\hline
-11x^2+\ 6x+\ 8\\
-(-11x^2+22x-44)\\
\hline
-16x+52
\end{array}
$$

V prvním řádku (před symbolem „:“) je výchozí hodnota polynomu z podle kroku (1). Sčítanec s nejvyšší mocninou polynomu z je $2x^5$ a ten podělíme prvním sčítancem polynomu q, tj. x^2. Výsledek zapíšeme vedle rovnítka: $2x^3$. Tímto výsledkem násobíme celý polynom q a píšeme pod výchozí polynom z do druhého řádku. Tyto dva polynomy odčítáme a výsledek píšeme pod čáru. Vzniká nová hodnota polynomu z. Sčítanec s nejvyšší mocninou je nyní x^4 a ten znovu dělíme x^2 a výsledek $+x^2$ připisujeme vedle rovnítka. Tímto výsledkem znovu násobíme celý polynom q a píšeme do čtvrtého řádku. Pod čáru zapíšeme do pátého řádku rozdíl, tedy novou hodnotu polynomu z. Postupujeme tak dlouho, dokud polynom z má stupeň větší nebo roven stupni polynomu q. Teprve na devátém řádku jsme dosáhli skutečného zbytku, neboť nyní tento polynom má stupeň menší než stupeň polynomu q. Výsledek částečného podílu můžeme zapsat takto:

$$\frac{2x^5-3x^4+3x^3-x^2-6x+8}{x^2-2x+4}=2x^3+x^2-3x-11+\frac{-16x+52}{x^2-2x+4}.$$

14.28. Definice. Nechť zbytek po dělení polynomu p polynomem q je nulový polynom. Pak říkáme, že *q dělí p* nebo že *p je dělitelný polynomem q*. Částečný podíl r v takovém případě nazýváme *podíl polynomů p a q* a značíme p/q.

14.29. Poznámka. Podíl polynomů p a q (pokud existuje) podle předchozí definice je polynom. Pokud bychom ovšem definovali podíl polynomů jako podíl funkcí, tj. takovou funkci

f, jejíž hodnoty $f(x)$ jsou rovny podílu $p(x)/q(x)$ všude tam, kde $q(x) \neq 0$, pak bychom nemuseli dostat polynom, protože definiční obor takové funkce f nemusí obsahovat všechna reálná čísla $\mathbf{R}$. Pravda, pokud je polynom p dělitelný polynomem q, pak funkci f lze spojitě dodefinovat v bodech x, pro které je $q(x) = 0$. Takto rozšířená funkce f je pak totožná s podílem polynomů podle předchozí definice ??. To plyne z následující věty.

14.30. Věta. Nechť polynom p je dělitelný polynomem q. Pak $(p/q)\, q = p$.

Důkaz. Polynom $(p/q) = r$ a $z = 0$ při značení podle věty ??. Pak dokazované tvrzení je vlastnost (i) uvedené věty.

14.31. Poznámka. Nechť je dán polynom p svými koeficienty $a_0, a_1, \ldots, a_n$. K nalezení hodnoty $p(\alpha)$ můžeme použít jednak vzorec (14.1)

$$p(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_2\alpha^2 + a_1\alpha + a_0 \tag{14.3}$$

nebo můžeme tento vzorec přezávorkovat do tvaru

$$p(\alpha) = ((\cdots((a_n\alpha + a_{n-1})\,\alpha + a_{n-2})\,\alpha + \cdots + a_2)\,\alpha + a_1)\,\alpha + a_0 \tag{14.4}$$

a hodnotu $p(\alpha)$ počítat postupně vyhodnocováním závorek od vnitřní k vnější. Snadno zjistíme (roznásobením závorek), že oba vzorce dávají skutečně tutéž hodnotu $p(\alpha)$, ovšem vzorec (14.4) je daleko méně numericky náročný. Představme si, že stupeň polynomu je 1524.

Podle vzorce (14.3) bychom museli počítat nejprve mocninu α^{1524}, zatímco vzorec (14.4) nás do ničeho takového nenutí.

Programátorští amatéři (kteří bohužel často fušují programátorům do řemesla) se poznají například podle toho, že pro vyhodnocení polynomu v bodě α použijí vzorec (14.3) a hloupě argumentují tím, že počítač je rychlý. Ano, je rychlý, ale jakmile bude potřeba vyhodnocovat tisíce polynomů v tisících různých bodech, a přitom ty polynomy budou mít stupeň kolem tisíce a bude potřeba tento postup opakovat, tak se přístup k programování hodně pozná. Na druhé straně opravdový programátor vyhodnotí polynom v bodě α podle vzorce (14.4) a využije k tomu ještě možnosti procesoru. Například do registru A uloží hodnotu α a registr B pronuluje a vyhradí pro mezivýpočty. Pak vyzvedne z paměti hodnotu a_n a přičte ji k B. Dále násobí A s B a výsledek uloží do B, dále vyzvedne z paměti a_{n-1} a přičte k B, pak opět násobí A s B a výsledek uloží do B, atd. K vyhodnocení polynomu stupně n v bodě α stačí provést n násobení a n sčítání.

Bohužel opravdových programátorů je málo, a proto software mnohdy vypadá jak vypadá. Uživatel pak nešťastně čeká u svého kompu a nemůže se dočkat výsledku. Hledí do blba, protože na blba, který to naprogramoval, nemá možnost se podívat. Často se mu také draze koupený software zhroutí, protože například postup podle vzorce (14.3) není numericky stabilní.

14.32. Poznámka. Budeme si hrát na pana Hornera, který používal vzorec (14.4) dávno před tím, než se objevily první počítače a který si zapisoval mezivýsledky do přehledného schématu. Záhy uvidíme, že ty mezivýsledky i ono přehledné schéma se budou hodit.

Označme obsah nejvíce vnitřní závorky ve vzorci (14.4) symbolem b_{n-2}, obsah další závorky označme b_{n-3} a tak dále až konečně poslední závorka (vnější) obklopuje výraz označený b_0. K tomu dopišme $b_{n-1} = a_n$. Pro mezivýsledky b_k tedy platí: $b_{n-1} = a_n$, $b_{k-1} = a_k + \alpha b_k$ pro $k = n-1, n-2, \dots, 3, 2, 1$. Celý výpočet hodnoty $p(\alpha)$ zapíšeme do třířádkového tzv. *Hornerova schématu*. V prvním řádku jsou koeficienty polynomu p a ve třetím řádku zmíněné mezivýpočty b_i.

	a_n	a_{n-1}	a_{n-2}	$\dots$	a_2	a_1	a_0
$\alpha:$		αb_{n-1}	αb_{n-2}	$\dots$	αb_2	αb_1	αb_0
	b_{n-1}	b_{n-2}	b_{n-3}	$\dots$	b_1	b_0	$p(\alpha)$

Schéma v druhém a třetím řádku plníme postupně zleva doprava tak, že do druhého řádku šikmo přepisujeme hodnotu třetího řádku násobenou α a následně směrem dolů sčítáme.

14.33. Příklad. Najdeme hodnotu polynomu $2x^8 - 3x^7 - 11x^6 + 5x^5 + 11x^3 - 2x^2 - 9x - 2$ v bodě 3 za použití Hornerova schématu.

	2	−3	−11	5	0	11	−2	−9	−2
$x = 3:$		6	9	−6	−3	−9	6	12	9
	2	3	−2	−1	−3	2	4	3	$7 = p(3)$

Do prvního řádku jsme nejdříve zapsali všechny koeficienty daného polynomu a nedopustili jsme se školácké chyby, že bychom zapomněli na koeficient $a_4 = 0$. Druhý řádek jsme nechali prázdný a udělali jsme sčítací čáru. Pod ní jsme přepsali číslo 2 ($b_7 = a_8$). Pak tuto dvojku násobíme trojkou (hodnotou x) a píšeme do druhého řádku následujícího sloupce: 6. Ve sloupci sčítáme. Dostáváme 3. Tuto trojku násobíme znovu hodnotou $x = 3$ a výsledek 9 píšeme do druhého řádku následujícího sloupce. Sčítáme, násobíme, sčítáme, násobíme atd. až nakonec dospíváme k číslu 7, což je hodnota daného polynomu v bodě $x = 3$.

14.34. Věta. Mezivýsledky b_i z Hornerova schématu jsou koeficienty částečného podílu polynomu p při dělení polynomem daným vzorcem $x - \alpha$. Zbytek tohoto dělení je konstantní polynom $p(\alpha)$.

Důkaz. Je $b_{n-1} = a_n$ a platí $b_{k-1} = a_k + \alpha b_k$ (neboli $a_k = b_{k-1} - \alpha b_k$) pro $k = n - 1, n-2, \ldots, 3, 2, 1$. Podle posledního sloupce Hornerova schématu je $a_0 + \alpha b_0 = p(\alpha)$, neboli $a_0 = p(\alpha) - \alpha b_0$. Tyto skutečnosti dosadíme do vzorce pro výpočet hodnoty polynomu p v bodě $x \in \mathbf{R}$:

$$\begin{aligned}
p(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = \\
&= b_{n-1}x^n + (b_{n-2} - \alpha b_{n-1})\, x^{n-1} + \cdots + (b_1 - \alpha b_2)x^2 + (b_0 - \alpha b_1)\, x + p(\alpha) - \alpha b_0 = \\
&= x\,(b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0) - \alpha\,(b_{n-1}x^{n-1} + \cdots + b_2 x^2 + b_1 x + b_0) + p(\alpha) = \\
&= (b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_2 x^2 + b_1 x + b_0)\,(x - \alpha) + p(\alpha).
\end{aligned}$$

14.35. Příklad. Najdeme částečný podíl a zbytek při dělení polynomu z příkladu ?? polynomem $x-3$. Podle předchozí věty je

$$\frac{2x^8-3x^7-11x^6+5x^5+11x^3-2x^2-9x-2}{x-3}=2x^7+3x^6-2x^5-x^4-3x^3+2x^2+4x+3+\frac{7}{x-3}.$$

Koeficienty částečného podílu jsme opsali z třetího řádku Hornerova schématu v příkladu ??. Toto je zřejmě méně pracná metoda hledání částečného podílu, než metoda popsaná v důkazu věty ??. Bohužel se tato metoda dá použít jen při dělení polynomu lineárním polynomem tvaru $x-\alpha$. Ovšem s dělením takovým lineárním polynomem se často setkáme například při rozkladu na kořenové činitele polynomu.

14.36. Poznámka. Až dosud jsme s polynomy pracovali jako s reálnými funkcemi reálné proměné případně jako se vzorečky, které mají reálné koeficienty a do kterých dosazujeme za formální proměnnou reálná čísla. Těmto polynomům říkáme *polynomy nad* **R**, neboli polynomy nad reálnými čísly.

Místo reálných čísel ale můžeme používat jakýkoli číselný obor, ve kterém umíme čísla mezi sebou sčítat, odčítat, násobit a dělit (podle jistých vlastností, podrobněji si o tom povíme v kapitole ??). Pokud budeme za polynom považovat komplexní funkci komplexní proměnné danou vzorečkem (14.2), ve kterém jsou koeficienty $a_0, a_1, \ldots, a_n$ komplexní čísla a za proměnou x dosazujeme komplexní čísla, mluvíme o *polynomu nad* **C**.

Pokud zaměníme slovo „reálný“ slovem „komplexní“ a symbol $\mathbf{R}$ symbolem $\mathbf{C}$ v celém předchozím textu v této kapitole, všechna tvrzení zůstávají v platnosti. Budeme-li v následujícím textu v této kapitole mluvit o polynomech a nespecifikujeme číselný obor, budeme předpokládat polynomy nad $\mathbf{C}$. Je to z toho důvodu, že budeme vyšetřovat vlastnosti kořenů polynomů. Reálné kořeny polynomů nad $\mathbf{R}$ přitom nemusejí existovat.

14.37. Definice. *Kořen polynomu* p je takové číslo $\alpha \in \mathbf{C}$, pro které je $p(\alpha) = 0$. Pokud α je kořen polynomu p, pak polynom daný vzorcem $x - \alpha$ pro všechna $x \in \mathbf{C}$ nazýváme *kořenový činitel polynomu* p.

14.38. Věta. Polynom p je dělitelný svým kořenovým činitelem.

Důkaz. Zbytek po dělení polynomu p polynomem $x-\alpha$ má podle věty ?? stupeň menší než 1, tedy jedná se o konstantu. Označme ji c. Pro všechna $x \in \mathbf{C}$ platí: $p(x) = r(x)\,(x-\alpha) + c$. Po dosazení $x = \alpha$ máme $p(\alpha) = r(\alpha) \cdot 0 + c = c$. Protože α je kořen, je $p(\alpha) = 0$, takže $c = 0$. Skutečně tedy polynom $x - \alpha$ dělí polynom p beze zbytku.

14.39. Poznámka. Nechť α_1 je kořen nenulového polynomu p. Zatím ponecháme stranou problém hledání kořene a spokojíme se s tím, že kořen polynomu p existuje a označíme jej α_1. Podle předchozí věty je možné dělit kořenovým činitelem, neboli $p(x) = r_1(x)\,(x-\alpha_1)$. Z této rovnosti plyne, že všechny kořeny polynomu r_1 jsou zároveň kořeny polynomu p. Polynom

p má kromě kořenů polynomu r_1 navíc jen kořen α_1. Je tedy možné hledat další kořeny polynomu p tak, že najdeme kořeny polynomu r_1. Přitom tento polynom má podle věty ?? o jedničku menší stupeň, než má polynom p.

Nechť α_2 je kořen polynomu r_1. Máme tedy $p(x) = r_2(x)\,(x-\alpha_1)\,(x-\alpha_2)$. Další kořeny polynomu p můžeme hledat tak, že najdeme kořeny polynomu r_2. Úvahu opakujeme tak dlouho, až se polynom r_i stane konstantním polynomem nebo až nastane situace, že polynom r_i nebude mít kořeny. Postup skončí určitě po konečně mnoha krocích, neboť stupně polynomu r_i se snižují. V závěru tedy máme

$$p(x) = r_m(x)\,(x-\alpha_1)\,(x-\alpha_2)\cdots(x-\alpha_m), \tag{14.5}$$

kde r_m je polynom bez kořenů (věta ?? ukáže, že takový případ nastává jen pro konstatní polynom) a α_i jsou všechny kořeny polynomu p. V zápise (14.5) se mohou některé kořeny α_i vyskytovat vícekrát. Takovým kořenům říkáme vícenásobné, viz následující definice.

14.40. Definice. Kořen α nenulového polynomu p nazýváme k-násobný, pokud polynom $(x-\alpha)^k$ dělí polynom p, a přitom polynom $(x-\alpha)^{k+1}$ nedělí polynom p. Občas je užitečné mluvit také o číslu α jako o 0-násobném kořenu polynomu p tehdy, když číslo α není kořenem polynomu p.

14.41. Věta. Nenulový polynom p má kořen α násobnosti k právě tehdy, když existuje polynom q tak, že $p(x) = (x-\alpha)^k q(x)$ a současně $q(\alpha) \neq 0$.

Důkaz. Protože $(x-\alpha)^k$ dělí polynom p právě tehdy, když existuje polynom q tak, že $p(x) = (x-\alpha)^k q(x)$ pro všechna $x \in \mathbf{C}$, stačí podle definice ?? dokázat, že $(x-\alpha)^{k+1}$ nedělí p právě když $q(\alpha) \neq 0$, neboli $(x-\alpha)^{k+1}$ dělí p právě když $q(\alpha) = 0$. Nechť $(x-\alpha)^{k+1}$ dělí p, tedy existuje polynom r tak, že $p(x) = (x-\alpha)^k (x-\alpha)\, r(x)$. Z jednoznačnosti podílu je zřejmé, že musí $q(x) = (x-\alpha)\, r(x)$, takže $q(\alpha) = 0$. Obráceně, pokud $q(\alpha) = 0$, pak podle věty ?? existuje polynom r tak, že $q(x) = (x-\alpha)\, r(x)$. Z toho plyne, že $p(x) = (x-\alpha)^k (x-\alpha)\, r(x)$, neboli $(x-\alpha)^{k+1}$ dělí p.

14.42. Příklad. Dejme tomu, že víme, že polynom $x^6 - 5x^5 - 15x^4 + 85x^3 + 10x^2 - 372x + 360$ má kořen 2. Určíme násobnost tohoto kořene.

Označme zkoumaný polynom písmenem p. Výpočtem hodnoty $p(2)$ za použití Hornerova schématu musí vyjít 0. Navíc třetí řádek schématu obsahuje podle věty ?? koeficienty polynomu r_1, pro který platí $p(x) = r_1(x)\,(x-2)$. Můžeme tedy tento řádek ztotožnit s prvním řádkem navazujícího Hornerova schématu, ve kterém ověřujeme, zda dvojka je kořenem polynomu r_1. Pokud zjistíme, že ano, pak už víme, že dvojka je aspoň dvojnásobným kořenem. V takovém případě můžeme pokračovat dalším navazujícím Hornerovým schématem až do

doby, než polynom r_i nebude mít kořen dvojku.

	1	−5	−15	85	10	−372	360
2 :		2	−6	−42	86	192	−360
	1	−3	−21	43	96	−180	0
2 :		2	−2	−46	−6	180	
	1	−1	−23	−3	90	0	
2 :		2	2	−42	−90		
	1	1	−21	−45	0		
2 :		2	6	−30			
	1	3	−15	−75			

Vidíme tedy, že $p(x) = (x^3+x^2-21x-45)(x-2)^3$. Přitom hodnota polynomu $x^3+x^2-21x-45$ pro $x = 2$ je -75, takže dvojka není kořenem tohoto polynomu. Číslo 2 je tedy trojnásobný kořen polynomu p.

Násobnost kořene tedy můžeme zjistit opakovaným použitím navazujícího Hornerova schématu, přičemž násobnost je počet výsledných řádků končících nulou s tím, že další řádek už nulou nekončí.

14.43. Poznámka. Hledat kořeny polynomu, neboli řešit algebraickou rovnici $p(x) = 0$, je úloha důležitá a v praxi často potřebná. Bohužel neexistuje obecný postup, jak na základě znalostí koeficientů polynomu $a_0, a_1, \ldots, a_n$ zjistit přesně kořeny tohoto polynomu. Postupy existují pro velmi speciální typy polynomů, například pro polynomy nízkých stupňů. V této poznámce připomeneme, jak je možné hledat kořeny polynomů nízkých stupňů.

-1) Kořeny polynomu stupně -1 (tedy nulového polynomu) jsou všechna komplexní čísla.

0) Polynom nultého stupně (tedy nenulová konstanta) nemá kořen.

1) Polynom prvního stupně $ax + b$ ($a \neq 0$, tzv. lineární polynom) má jeden kořen $-b/a$.

2) Polynom druhého stupně $ax^2 + bx + c$ ($a \neq 0$, nazývaný též kvadratický polynom) má dva kořeny $(-b + \sqrt{b^2 - 4ac})/2a, (-b - \sqrt{b^2 - 4ac})/2a$. Je-li $b^2 - 4ac = 0$, jedná se o jeden dvojnásobný kořen.

3) Polynom třetího stupně (tzv. kubický polynom) má tři kořeny, které lze z koeficientů polynomu spočítat pomocí tzv. Cardanových vzorců. Tyto vzorce je možné dohledat v matematických tabulkách (například [3] nebo [25]), ovšem pro jejich přílišnou komplikovanost se s nimi člověk často nesetká. Používají se jen v některých počítačových programech často bez vědomí uživatele.

4) Polynom čtvrtého stupně má čtyři kořeny, které lze spočítat z koeficientů polynomu pomocí vzorců, jež je možné dohledat v tabulkách. Ani v tomto případě se s těmito vzorci často nesetkáváme.

5) Pro polynomy pátého a vyššího stupně neexistují obecné vzorce pro výpočet kořenů z koeficientů polynomu. Není pravda, že by v budoucnu někdo tyto vzorce mohl objevit. Niels Abel totiž dokázal, že je to nemožné.

Příroda nám prostřednictvím Abela uštědřila další lekci: poodhalila nám své tajemství, které v tomto případě zní: v určitých partiích jsem neodhalitelná.

Je potřeba si uvědomit, že neexistence vzorců pro výpočet kořenů polynomů stupně pátého a vyššího nemá co dělat s existencí nebo neexistencí těch kořenů samotných. Matematik občas pracuje s faktem, že dokáže něčeho existenci a současně dokáže, že to co existuje, neumí spočítat. Tak je tomu i v tomto případě, jak za chvíli ukáže fundamentální věta algebry ??.

14.44. Příklad. Uvažujme tzv. *binomickou rovnici*, tj. rovnici tvaru $x^n - a = 0$, kde $n > 0$ je přirozené číslo a $a \in \mathbf{C}$. Řešení této rovnice jsou všechny kořeny polynomu $x^n - a$. To je další speciální typ polynomu, u kterého umíme najít všechny kořeny, dokonce pro libovolný stupeň takového polynomu.

Binomickou rovnici $x^n - a = 0$ přepíšeme do tvaru $x^n = a$ a odmocníme, tj. formálně dostáváme $x = \sqrt[n]{a}$. Úkolem je najít všechny n-té odmocniny z komplexního čísla a. Toto číslo zapíšeme ve tvaru $a = |a|\,(\cos\alpha + i\sin\alpha)$, kde $|a|$ je velikost čísla a a α je úhel v rovině komplexních čísel mezi kladnou reálnou osou a polopřímkou s počátkem v bodě 0 procházející

bodem a (tzv. *argument* komplexního čísla a). S využitím Moivreovy věty dostáváme

$$\left(\sqrt[n]{|a|}\left(\cos\frac{\alpha+2k\pi}{n}+i\sin\frac{\alpha+2k\pi}{n}\right)\right)^n=|a|\left(\cos(\alpha+2k\pi)+i\sin(\alpha+2k\pi)\right)=a$$

pro všechna $k\in\{0,1,2,\ldots,n-1\}$. Takže komplexní čísla

$$\sqrt[n]{|a|}\left(\cos\frac{\alpha+2k\pi}{n}+i\sin\frac{\alpha+2k\pi}{n}\right)$$

jsou pro $k\in\{0,1,2,\ldots,n-1\}$ různé n-té odmocniny z čísla a. Všechna tato čísla řeší danou binomickou rovnici. Ze vzorce (14.5) plyne, že polynom stupně n má nejvýše n kořenů, takže uvedené n-té odmocniny z čísla a jsou *všechny* kořeny polynomu x^n-a.

14.45. Věta (fundamentální věta algebry). Každý polynom stupně aspoň prvého má v $\mathbb{C}$ kořen.

Důkaz. Tato věta je jednoduchým důsledkem složitějších výsledků z komplexní analýzy. Většinou se tedy důkaz věty v prvních semestrech vysokoškolského studia neuvádí s poukazem na to, že věta bude dokázána později. Z tohoto pohledu se mi líbí důkaz uvedený v [24], který se opírá o relativně jednoduchou matematiku. Důkaz zde skoro doslova přepisuji včetně některého značení (písmeno ξ čteme ksí). Připouštím, že ke čtení potřebuje být čtenář v pohodě

a bez spěchu. Chci proto naléhavě upozornit, že následující pasáž textu je určena jen pro hloubavého čtenáře. Ostatní čtenáři přejdou rovnou k poznámce ??.

V důkazu věty budeme na mnoha místech používat $|xy| = |x|\,|y|$ pro $x, y \in \mathbf{C}$. Tuto vlastnost můžeme ověřit převedením komplexních čísel na tvar $x = |x|\,e^{i\alpha}, y = |y|\,e^{i\beta}$ a využitím faktu, že $\left|e^{i(\alpha+\beta)}\right| = 1$ (což plyne z Moivreovy věty, viz ??).

Dále často použijeme trojúhelníkovou nerovnost, tedy $|x+y| \le |x| + |y|$ pro $x, y \in \mathbf{C}$. Ověříme např. při značení $x = a+ib, y = c+id$. $|x+y|^2 = (a+c)^2 + (b+d)^2 = a^2+b^2+c^2+d^2+2ac+2bd$, $(|x|+|y|)^2 = a^2+b^2+2\sqrt{(a^2+b^2)(c^2+d^2)}+c^2+d^2$. Po odečtení a druhém umocnění máme dokázat $(ac+bd)^2 \le (a^2+b^2)(c^2+d^2)$, což plyne z nerovnosti $0 \le (ad-bc)^2$.

K důkazu fundamentální věty algebry použijeme tři pomocné věty (lemmata):

14.46. Věta. Nechť p je polynom stupně aspoň prvého. Pak $\lim |p(x)| = +\infty$ pro $|x| \to +\infty$, neboli $\forall K \ge 0\ \exists r > 0$ tak, že pro všechna $x \in \mathbf{C}$, pro něž $|x| > r$, platí $|p(x)| > K$.

Důkaz. Nechť p má koeficienty $a_0, a_1, \ldots, a_n$, $n \ge 0$, $a_n \neq 0$. Pro $x \in \mathbf{C}$ je

$$|a_n x^n| = \left|p(x) - (a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)\right| \le |p(x)| + |a_{n-1}x^{n-1}| + \cdots + |a_1 x| + |a_0|,$$

takže pro $x \neq 0$ je

$$|p(x)| \ge |a_n||x|^n - \cdots - |a_1|\,|x| - |a_0| = |x|^n \left(|a_n| - \frac{|a_{n-1}|}{|x|} - \cdots - \frac{|a_1|}{|x|^{n-1}} - \frac{|a_0|}{|x|^n}\right).$$

Pokud $|x| \to +\infty$, pak $|p(x)| \to +\infty$, protože závorka v posledním výrazu má limitu $|a_n| \neq 0$.

14.47. Věta. Nechť p je polynom stupně aspoň prvého. Pak funkce $|p| : \mathbf{C} \to \mathbf{R}$ definovaná vztahem $|p|(x) = |p(x)|$ má lokální minimum na $\mathbf{C}$.

Důkaz. Označme $K = |p(0)| + 1$. Podle předchozí věty existuje $r > 0$ tak, že $|p(x)| > K$ pro všechna $x \in \mathbf{C}, |x| > r$. Označme $S_r = \{x \in \mathbf{C};\ |x| \leq r\}$, tj. kroužek komplexních čísel o poloměru r se středem 0. Na okraji kroužku S_r je $|p(x)| \geq K$, protože $|p|$ je spojitá a vně kroužku má hodnoty větší než K. Protože S_r je omezený a kompaktní, dosahuje spojitá funkce $|p|$ na S_r svého minima. Toto minimum je menší než K, protože $0 \in S_r$ a $|p(0)| = K - 1$. Takže minimum leží uvnitř kroužku S_r a jde o lokální minimum funkce $|p|$ na $\mathbf{C}$.

14.48. Věta. Nechť p je polynom stupně aspoň prvého. Nechť číslo $x_0 \in \mathbf{C}$ je zvoleno tak, že $|p(x_0)| > 0$. Potom funkce $|p| : \mathbf{C} \to \mathbf{R}$ nemá lokální minimum v x_0.

Jinými slovy, existuje $\xi \in \mathbf{C}$ (komplexní číslo určující směr, ve kterém $|p|$ klesá) tak, že pro dostatečně malé $t > 0$ je $|p(x_0 + t\xi)| < |p(x_0)|$.

Důkaz. Označme $c = p(x_0) \neq 0$. Polynom daný vzorcem $p(x) - c$ je z předpokladu o stupni p nenulový. Číslo x_0 je kořenem polynomu $p - c$ a nechť m je násobnost x_0. Je $m \geq 1$ a podle věty ?? polynom $(x - x_0)^m$ dělí polynom $p - c$, neboli existuje nenulový polynom q tak, že $p(x) - c = (x - x_0)^m q(x)$ pro všechna $x \in \mathbf{C}$. Označme $d = q(x_0) \neq 0$.

Volme $\xi \in \mathbf{C}$ tak, aby $\xi^m = -\frac{c}{d}$. To je možné, stačí najít nějakou m-tou odmocninu z komplexního čísla $-\frac{c}{d}$, viz příklad ??. Je tedy $\xi^m \frac{d}{c} = -1$.

Pro $t \in \mathbf{R}$ počítejme $p(x_0 + t\xi)$:

$$p(x_0+t\xi) = c+(t\xi)^m q(x_0+t\xi) = c+(t\xi)^m \big(q(x_0+t\xi)-d+d\big) = c+t^m\xi^m d+t^m\xi^m \big(q(x_0+t\xi)-d\big).$$

Poslední závorku označíme $r(t) = q(x_0 + t\xi) - d$, tj. $r : \mathbf{R} \to \mathbf{C}$ je polynom. Nechť $b_0, b_1, \ldots, b_s$ jsou jeho koeficienty. Protože $r(0) = 0$ (viz $d = q(x_0)$), je $b_0 = 0$, takže $r(t) = t(b_1 + b_2 t + \cdots + b_s t^{s-1})$.

Najdeme $K \geq 0$ takové, že $|r(t)| \leq Kt$ pro všechna $t \in \langle 0, 1\rangle$. To se podaří, protože pro $t \in \langle 0, 1\rangle$ je $|r(t)| = |t|\,|b_1 + \cdots + b_s t^{s-1}| \leq |t|(|b_1| + \cdots + |b_s t^{s-1}|) = |t|(|b_1| + \cdots + |b_s|\,t^{s-1}) \leq |t|(|b_1| + \cdots + |b_s|)$, takže stačí volit $K = |b_1| + \cdots + |b_s|$. Vraťme se k počítání $p(x_0 + t\xi)$. Využijeme rovnost $\xi^m \frac{d}{c} = -1$.

$$p(x_0+t\xi) = c+t^m\xi^m d+t^m\xi^m r(t) = c\left(1 + t^m\xi^m\frac{d}{c} + t^m\xi^m\frac{r(t)}{c}\right) = c\left(1 - t^m + t^m\xi^m\frac{r(t)}{c}\right),$$

takže $|p(x_0+t\xi)| = |c|\,\left|1 - t^m + t^m\xi^m\frac{r(t)}{c}\right|$. Cílem je ukázat, že posledně jmenovaná absolutní hodnota je menší než 1 pro malá kladná t. Využijeme odhad $|r(t)| \leq Kt$:

$$\left|1 - t^m + t^m\xi^m\frac{r(t)}{c}\right| \leq |1 - t^m| + \left|t^m\xi^m\frac{Kt}{c}\right| = 1 - t^m + t^{m+1}K\left|\frac{\xi^m}{c}\right| = 1 + t^m\left(tK\left|\frac{\xi^m}{c}\right| - 1\right).$$

Pro dostatečně malá $t > 0$ je poslední závorka blízká číslu -1, tedy záporná, takže uvedený výraz jako celek je menší než 1.

Důkaz fundamentální věty algebry ??. Podle věty ?? funkce $|p| : \mathbf{C} \to \mathbf{R}$ nabývá svého lokálního minima. Podle věty ?? toto minimum není v bodě, ve kterém $|p(x)| > 0$. Protože $|p(x)| \geq 0$, musí být hledané minimum v bodě $x \in \mathbf{C}$, pro které je $|p(x)| = 0$, tj. $p(x) = 0$. Existence kořenu je dokázána.

14.49. Poznámka. Důsledkem věty ?? je skutečnost, že polynom r_m ve vzorci (14.5) je konstantní. Z toho a z věty ?? také plyne, že polynom p má ve vzorci (14.5) tolik kořenových činitelů, kolik je jeho stupeň. Počítáme-li tedy každý kořen tolikrát, kolik je jeho násobnost, můžeme říci, že polynom má stejný počet kořenů, jako je jeho stupeň. Konečně, protože $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m) = 1x^m + \cdots$, musí být konstantní polynom r_m roven koeficientu a_m, což je nenulový koeficient u nejvyšší mocniny polynomu p. Všechny tyto poznatky zformulujeme do následující věty.

14.50. Věta. Nechť p je nenulový polynom stupně n s koeficienty $a_0, a_1, \ldots, a_n$ a nechť $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathbf{C}$ jsou všechny jeho navzájem různé kořeny. Nechť k_i je násobnost kořenu α_i pro $i \in \{1, 2, \ldots, s\}$. Pak platí $k_1 + k_2 + \cdots + k_s = n$ a dále pro všechna $x \in \mathbf{C}$ je

$$p(x) = a_n\,(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_s)^{k_s}.$$

Tomuto zápisu říkáme *rozklad polynomu na kořenové činitele*.

Důkaz. Viz poznámku ??.

14.51. Věta. Nenulový polynom stupně n má nejvýše n různých komplexních kořenů.

Důkaz. Věta je přímým důsledkem věty ??.

14.52. Věta. Pokud se dva polynomy stupně nejvýše n shodují v $n+1$ různých bodech, pak jsou totožné. Jinými slovy, polynom stupně n je jednoznačně určen svými hodnotami v $n+1$ bodech.

Důkaz. Předpokládáme, že pro polynomy p a q existují vzájemně různá čísla $\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1}$ taková, že $p(\alpha_i) = q(\alpha_i)$ pro $i \in \{1, 2, \ldots, n, n+1\}$. Protože polynomy p a q mají stupeň nejvýše n, je podle věty ?? rozdíl $p - q$ polynom stupně nejvýše n, který má kořeny $\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1}$. Těch kořenů je více, než je jeho stupeň. To podle věty ?? není možné jinak, než že je polynom $p - q$ nulový. Takže $p = q$ a důkaz je hotov.

14.53. Poznámka. Bude následovat několik modelových příkladů na rozklad polynomu na kořenové činitele. Je potřeba si uvědomit, že tyto příklady jsou schválně voleny tak, aby se povedlo kořeny uhádnout. Poznámka ?? ale mluví jasně: moc možností při hledání kořenů

nemáme. Modelové příklady na hledání kořenů jsou často typické tím, že se dá uhádnout kořen jako malé celé číslo nebo jednoduchý zlomek. Abychom mohli hádat jen z konečně mnoha možností, využijeme následující dvě věty.

14.54. Věta. Nechť polynom p má celočíselné koeficienty $a_0, a_1, \ldots, a_n$. Je-li α celočíselným kořenem polynomu p, pak α dělí koeficient a_0.

Důkaz. Věta je speciálním případem následující věty pro $d = 1$.

14.55. Věta. Nechť polynom p stupně n má celočíselné koeficienty $a_0, a_1, \ldots, a_n$. Je-li $\alpha = \frac{c}{d}$ racionálním kořenem polynomu p a čísla c, d jsou celá nesoudělná, pak c dělí a_0 a d dělí a_n.

Důkaz. Protože $\frac{c}{d}$ je kořen, platí

$$a_0 + a_1 \frac{c}{d} + a_2 \left(\frac{c}{d}\right)^2 + \cdots + a_n \left(\frac{c}{d}\right)^n = 0.$$

Po převedení a_0 na druhou stranu rovnosti, vynásobení rovnosti číslem d^n a vytknutí čísla c dostáváme

$$c\,(a_1 d^{n-1} + a_2 c d^{n-2} + a_3 c^2 d^{n-3} + \cdots + a_n c^{n-1}) = -a_0 d^n.$$

Číslo $e = -d^n$ je nesoudělné s c a uvedená závorka obsahuje celé číslo, které označíme k. Výše uvedená rovnost má tvar $c \cdot k = a_0 \cdot e$. Číslo c tedy musí dělit a_0. Nyní vyjádříme z původní rovnosti a_n:

$$d\,(a_0 d^{n-1} + a_1 c d^{n-2} + a_2 c^2 d^{n-3} + \cdots + a_{n-1} c^{n-1}) = -a_n c^n.$$

Podobnou úvahou jako před chvílí dospíváme k závěru, že d musí dělit a_n.

14.56. Příklad. Najdeme rozklad na kořenové činitele polynomu z příkladu ??, který je dán vzorcem

$$p(x) = x^6 - 5x^5 - 15x^4 + 85x^3 + 10x^2 - 372x + 360.$$

Podle věty ?? je možno celočíselné kořeny hledat jen mezi děliteli čísla 360. Bohužel dělitelů čísla 360 je mnoho. Čtenář si za domácí cvičení zkusí všechny dělitele vypsat. Shledá, že jich je 48, pokud ovšem nezapomene zapsat i záporné dělitele. Obvykle začínáme dosazovat takové dělitele, které jsou v absolutní hodnotě co nejmenší. Tedy $p(1) = 64$ (není kořen), $p(-1) = 648$ (není kořen), $p(2) = 0$ (ejhle, je to kořen)! Navíc, jak ukazuje příklad ??, je tento kořen dokonce trojnásobný, takže s využitím výsledku toho příkladu máme $p(x) = (x^3+x^2-21x-45)(x-2)^3$.

Další kořeny polynomu p jsou určitě i kořeny polynomu $x^3 + x^2 - 21x - 45$. Dále tedy hledáme kořeny jen tohoto kubického polynomu r. Hádáme dále celá čísla (protože v modelových příkladech nás nikdo nebude nutit použít Cardanovy vzorce). Stačí se omezit na dělitele čísla 45, tedy na čísla z množiny $\{-45, -15, -9, -5, -3, -1, 1, 3, 5, 9, 15, 45\}$. Jedničku a mínus

jedničku už jsme testovali s negativím výsledkem v případě polynomu p, nemusíme ji tedy zkoušet znovu. Vyzkoušíme $r(3) = -72$ (není kořen), $r(-3) = 0$ (ejhle kořen)! Hornerovo schéma pro -3 vypadá takto:

$$\begin{array}{rrrrr} & 1 & 1 & -21 & -45 \\ -3: & & -3 & 6 & 45 \\ \hline & 1 & -2 & -15 & 0 \\ -3: & & -3 & 15 & \\ \hline & 1 & -5 & 0 & \end{array}$$

Vidíme, že číslo -3 je dvojnásobný kořen a že je $x^3 + x^2 - 21x - 45 = (x+3)^2(x-5)$, takže 5 je poslední kořen vyšetřovaného polynomu. Máme rozklad:

$$x^6 - 5x^5 - 15x^4 + 85x^3 + 10x^2 - 372x + 360 = (x-2)^3(x+3)^2(x-5).$$

Polynom p má tedy následující kořeny: 2 (trojnásobný kořen), -3 (dvojnásobný kořen) a 5 (jednonásobný kořen).

14.57. Příklad. Najdeme rozklad polynomu $3x^6 - 8x^5 + 22x^4 + 54x^3 - 5x^2 - 26x$ na kořenové činitele.

Označme vyšetřovaný polynom písmenem p. Především, tento polynom má koeficient $a_0 = 0$, takže nula je kořenem polynomu. Kořenový činitel $x - 0$ píšeme stručně jako x a vznikne jednoduše vytknutím proměnné x ze zadaného výrazu:

$$p(x) = x\,(3x^5 - 8x^4 + 22x^3 + 54x^2 - 5x - 26).$$

Dále stačí najít rozklad polynomu $3x^5 - 8x^4 + 22x^3 + 54x^2 - 5x - 26$, který označíme q. Nejprve hádáme celočíselné kořeny mezi děliteli čísla 26: $q(1) = 40$ (není kořen), $q(-1) = 0$ (ejhle, kořen)! Navazujícím Hornerovým schématem vyzkoumáme jeho násobnost:

	3	−8	22	54	−5	−26
−1 :		−3	11	−33	−21	26
	3	−11	33	21	−26	0
−1 :		−3	14	−47	26	
	3	−14	47	−26	0	
−1 :		−3	17	−64		
	3	−17	64	−90		

Číslo -1 je tedy dvojnásobným kořenem a máme $q(x) = (x+1)^2(3x^3 - 14x^2 + 47x - 26)$ Dále budeme rozkládat uvedený kubický polynom, který označíme r. Pokračujeme ve zkoumání

dělitelů čísla 26: $r(2) = 36$ (není kořen), $r(-2) = -200$ (není kořen), $r(13) = 4810$ (není kořen), $r(-13) = -9594$ (není kořen), $r(26) = 44460$ (není kořen), $r(-26) = -63440$ (není kořen). Z věty ?? plyne, že polynom r nemá žádný celočíselný kořen. Protože koeficient u nejvyšší mocniny je $a_3 = 3 \neq 1$, podle věty ?? je možné, že kořenem bude zlomek, jehož čitatel dělí 26 a jmenovatel dělí 3. Vyzkoušíme $r(1/3) \doteq -11{,}777$ (není kořen), $r(-1/3) \doteq -43{,}333$ (není kořen), $r(2/3) = 0$ (ejhle kořen)! Pomocí Hornerova schématu můžeme najít rozklad:

	3	−14	47	−26
2/3 :		2	−8	26
	3	−12	39	0

Takže $r(x) = (x - \frac{2}{3})(3x^2 - 12x + 39)$. Kořeny kvadratického polynomu umíme najít:

$$\frac{12 \pm \sqrt{144 - 468}}{6} = \frac{12 \pm i\sqrt{324}}{6} = \frac{12 \pm 18i}{6} = 2 \pm 3i.$$

Hledaný rozklad tedy je

$$p(x) = 3x\,(x+1)^2(x - \tfrac{2}{3})(x - 2 + 3i)(x - 2 - 3i).$$

Povšimněte si, že v rozkladu je kromě kořenových činitelů uveden koeficient u nejvyšší mocniny a_6 polynomu p. Na něj nesmíme zapomenout. Polynom p má nulu jako jednonásobný kořen, -1 je dvojnásobný kořen, $\frac{2}{3}$ je jednonásobný kořen a konečně čísla $2 + 3i$ a $2 - 3i$ jsou vzájemně komplexně sdružené jednonásobné kořeny.

14.58. Příklad. Pokusíme se najít rozklad na kořenové činitele polynomu z příkladu ??, tedy

$$p(x) = 2x^8 - 3x^7 - 11x^6 + 5x^5 + 11x^3 - 2x^2 - 9x - 2.$$

Pokud má tento polynom racionální kořeny, pak podle věty ?? jejich čitatel musí dělit dvojku a jmenovatel musí také dělit dvojku. Kořeny budeme tedy hádat z množiny $\{-2, -1, -\frac{1}{2}, \frac{1}{2}, 1, 2\}$. Pusťme se do toho: $p(1) = -9$ (není kořen), $p(-1) = -17$ (není kořen), $p(2) = -356$ (není kořen), $p(-2) = -48$ (není kořen), $p(1/2) \doteq -5{,}656$ (není kořen), $p(-1/2) \doteq 0{,}328$ (není kořen). Zjistili jsme, že tento polynom nemá racionální kořeny. Podle fundamentální věty algebry ?? tento polynom kořen má, podle jednoduchých důsledků této věty tento polynom dokonce má osm kořenů, pokud každý počítáme tolikrát, kolik je jeho násobnost. Tyto kořeny jsou zřejmě iracionální čísla nebo se jedná o komplexní kořeny s nenulovou imaginární částí. Bohužel, ani jeden takový kořen neumíme najít, ačkoli koeficienty toho polynomu vypadají celkem nevinně (jsou to malá celá čísla). Můžeme tedy pouze prohlásit, že rozklad na kořenové činitele tohoto polynomu existuje, ale nevíme, jak tento rozklad vypadá.

Chtěl bych velmi upozornit, že toto je obvyklý jev. Pokud náhodně vybereme z osudí, ve kterém jsou všechny polynomy, jeden, pak skoro jistě neumíme najít jeho kořeny. Desítky, možná stovky, příkladů, které se vyskytují v učebnicích základního kurzu o polynomech, jsou vyumělkované a voleny tak, aby bylo možné nějak kořeny najít. Daleko typičtější je ovšem příklad tento: kořeny najít neumíme.

V praxi se můžeme setkat navíc s polynomy vysokých stupňů, jejichž koeficienty ani nejsou celá čísla. Pak si můžeme být skoro jisti, že kořeny najít nelze. Protože ale úloha

rozkladu na kořenové činitele a hledání kořenů je pro další výpočty většinou potřebná, je nutné přistoupit k hledání kořenů alespoň přibližně numerickými metodami. Tato problematika ale nespadá do náplně tohoto textu.

Pro ilustraci jsem použil řešítko v Maple, které má v sobě zabudovány numerické metody hledání kořenů. Pro daný polynom vyšel tento přibližný výsledek:

$$x_1 \doteq -2{,}05376, \quad x_2 \doteq -0{,}55262, \quad x_3 \doteq -0{,}25957, \quad x_4 \doteq 2{,}99882,$$
$$x_{5,6} \doteq -0{,}26936 \pm 1{,}00279\,i, \quad x_{7,8} \doteq 0{,}95292 \pm 0{,}37662\,i,$$
$$p(x) = 2\,(x-x_1)\,(x-x_2)\,(x-x_3)\,(x-x_4)\,(x-x_5)\,(x-x_6)\,(x-x_7)\,(x-x_8).$$

14.59. Příklad. Najdeme rozklad polynomu $x^n - a$ na kořenové činitele.

Využijeme výsledku příkladu ??. Rozklad na kořenové činitele je

$$x^n - a = \prod_{k=0}^{n-1} \left(x - \sqrt[n]{|a|} \left(\cos \frac{\alpha + 2k\pi}{n} + i \sin \frac{\alpha + 2k\pi}{n} \right) \right), \tag{14.6}$$

kde symbol $\prod$ značí součin výrazů, které následují, pro k od nuly do $n-1$.

14.60. Příklad. Najdeme rozklad polynomu $x^8 - 1$ na kořenové činitele.

Je potřeba najít osmé odmocniny z jedné. Jedničku pišme jako $1 = 1\,e^{i(0+2k\pi)}$. Všechny kořeny jsou ve tvaru

$$\sqrt[8]{1} = e^{i\frac{2k\pi}{8}} = \cos\frac{k\pi}{4} + i\sin\frac{k\pi}{4}, \quad k \in \{0,1,2,3,4,5,6,7\}.$$

Pro $k = 0$ je $\sqrt[8]{1} = 1$, pro $k = 1$ a $k = 7$ je $\sqrt[8]{1} = \frac{\sqrt{2}}{2} \pm i\frac{\sqrt{2}}{2}$, pro $k = 2$ a $k = 6$ je $\sqrt[8]{1} = \pm i$, pro $k = 3$ a $k = 5$ je $\sqrt[8]{1} = -\frac{\sqrt{2}}{2} \pm i\frac{\sqrt{2}}{2}$ a konečně pro $k = 4$ je $\sqrt[8]{1} = -1$. Z tohoto hlediska je nutno tento příklad považovat za modelový, neboť potřebné hodnoty funkcí sinus a kosinus byly tabulkové. Kdybychom počítali např. $\sqrt[7]{1}$, tabulkových hodnot bychom nemohli využít a museli bychom nechat výsledek ve tvaru (14.6) nebo jej vyčíslit numericky. Rozklad polynomu $x^8 - 1$ na kořenové činitele je

$$x^8-1 = (x-1)\left(x-\tfrac{\sqrt{2}}{2}-i\tfrac{\sqrt{2}}{2}\right)\left(x-\tfrac{\sqrt{2}}{2}+i\tfrac{\sqrt{2}}{2}\right)(x-i)(x+i)\left(x+\tfrac{\sqrt{2}}{2}-i\tfrac{\sqrt{2}}{2}\right)\left(x+\tfrac{\sqrt{2}}{2}+i\tfrac{\sqrt{2}}{2}\right)(x+1).$$

14.61. Poznámka. V příkladech ??, ??, ?? vyšly komplexní kořeny vzájemně po dvou komplexně sdružené. Následující věty ukazují, že se nejedná o náhodu, ale pro polynomy s reálnými koeficienty je to zákonitá vlastnost.

14.62. Věta. Je-li α kořen polynomu p s reálnými koeficienty, pak komplexně sdružené číslo $\overline{\alpha}$ je také kořenem polynomu p.

Důkaz. Připomenu, že komplexně sdružené číslo značíme pruhem nad číslem a definujeme jako číslo s opačnou imaginární částí, tj. $\overline{a+ib} = a-ib$. Dále je potřeba připomenout základní vlastnosti:

$x = \overline{x}$ právě když $x \in \mathbf{R}$, protože $\overline{a+0i} = a - 0i = a$.
$\overline{x} + \overline{y} = \overline{x+y}$, protože $\overline{a+ib} + \overline{c+id} = a + c - i(b+d) = \overline{a+ib+c+id}$.
$\overline{x}\,\overline{y} = \overline{xy}$, protože $(a-ib)(c-id) = ac - bd - i(bc+ad) = \overline{ac-bd+i(bc+ad)} = \overline{(a+ib)(c+id)}$.
$\overline{x^n} = \overline{x}^n$, protože $\overline{x} \cdot \overline{x^{n-1}} = \overline{x\,x^{n-1}} = \overline{x^n}$.

Jelikož α je kořen, platí $p(\alpha) = 0$. Máme dokázat, že $p(\overline{\alpha}) = 0$.

$$\begin{aligned} p(\overline{\alpha}) &= a_0 + a_1\overline{\alpha} + a_2\overline{\alpha}^2 + \cdots + a_n\overline{\alpha}^n = \overline{a_0} + \overline{a_1}\,\overline{\alpha} + \overline{a_2}\,\overline{\alpha}^2 + \cdots + \overline{a_n}\,\overline{\alpha}^n = \\ &= \overline{a_0} + \overline{a_1}\,\overline{\alpha} + \overline{a_2}\,\overline{\alpha^2} + \cdots + \overline{a_n}\,\overline{\alpha^n} = \overline{a_0} + \overline{a_1\,\alpha} + \overline{a_2\,\alpha^2} + \cdots + \overline{a_n\,\alpha^n} = \\ &= \overline{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n} = \overline{p(\alpha)} = \overline{0} = 0. \end{aligned}$$

Nejprve jsme využili toho, že koeficienty $a_0, a_1, \ldots, a_n$ jsou reálné. Další rovnosti plynou ze základních vlastností komplexně sdruženého čísla.

Věta nevylučuje případ, že α je reálný kořen. Pak ale $\overline{\alpha} = \alpha$, což je také (tentýž) kořen.

14.63. Věta. Nechť α je kořen nenulového polynomu p s reálnými koeficienty. Pak kořeny α a $\overline{\alpha}$ mají stejnou násobnost.

Důkaz. Předpokládejme, že násobnost kořene α je k a násobnost $\overline{\alpha}$ je k'. Bez újmy na obecnosti je možno předpokládat $k \leq k'$. V rozkladu na kořenové činitele polynomu p se vyskytuje kromě $(x-\alpha)$ také činitel $(x-\overline{\alpha})$. Součin těchto dvou činitelů

$$(x-\alpha)(x-\overline{\alpha}) = (x-a-ib)(x-a+ib) = x^2 - 2ax + a^2 + b^2$$

je polynom s reálnými koeficienty. Označme jej q. Polynom q^k má také reálné koeficienty a navíc dělí polynom p beze zbytku. Označme $p/q = r$. Polynom r má (díky algoritmu pro dělení polynomu polynomem) reálné koeficienty. Nemůže se tedy stát, aby r měl jen kořen $\overline{\alpha}$, a přitom neměl kořen α. Násobnosti tedy musejí být stejné.

14.64. Poznámka. Pokud je dán polynom s reálnými koeficienty, pak podle předchozí věty má stejný počet kořenových činitelů tvaru $x-\alpha$ jako činitelů tvaru $x-\overline{\alpha}$. Tyto činitele můžeme po dvou roznásobit a vytvořit tak kvadratické polynomy s reálnými koeficienty

$$(x-\alpha)\,(x-\overline{\alpha}) = (x-a-ib)\,(x-a+ib) = x^2 - 2ax + a^2 + b^2 = x^2 + cx + d.$$

Tím se v rozkladu na součin polynomů vyhneme práci s komplexními čísly. To může být pro uživatele, který pracuje s reálnými polynomy a očekává tedy reálné rozklady, důležité. Zformulujeme proto větu o reálném rozkladu na součin polynomů.

14.65. Věta. Nechť nenulový polynom p stupně n má reálné koeficienty. Nechť $\alpha_1, \alpha_2, \ldots, \alpha_s$ jsou všechny jeho vzájemně různé reálné kořeny s násobnostmi po řadě $k_1, k_2, \ldots, k_s$. Nechť $\beta_1, \overline{\beta_1}, \ldots, \beta_t, \overline{\beta_t}$ jsou všechny vzájemně různé komplexní kořeny polynomu p s nenulovou imaginární částí, které mají v souladu s větou ?? násobnosti po řadě $r_1, r_1, r_2, r_2, \ldots, r_t, r_t$. Pak je

$$n = k_1 + k_2 + \cdots + k_s + 2\,(r_1 + r_2 + \cdots + r_t)$$

a existují reálná čísla c_i, d_i, pro $i \in \{1, \ldots, t\}$ tak, že pro všechna $x \in \mathbf{R}$ je

$$p(x) = a_n\,(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_s)^{k_s}(x^2+c_1x+d_1)^{r_1}(x^2+c_2x+d_2)^{r_2}\cdots(x^2+c_ux+d_t)^{r_t}.$$

Uvedený vzorec se nazývá *reálný rozklad polynomu p*.

Důkaz. Je $(x-\beta_i)(x-\overline{\beta_i}) = x^2 + c_ix + d_i$, viz poznámku ??. Vše ostatní plyne z věty ??.

14.66. Příklad. Rozklad na kořenové činitele v příkladu ?? je současně reálným rozkladem, protože polynom nemá komplexní kořeny s nenulovou imaginární částí.

Polynom z příkladu ?? má reálný rozklad $p(x) = 3x\,(x+1)^2(x-\frac{2}{3})\,(x^2-4x+13)$.

Polynom z příkladu ?? má reálný rozklad $p(x) = (x-1)\,(x+1)\,(x^2+1)\,(x^2+\sqrt{2}\,x+1)\,(x^2-\sqrt{2}\,x+1)$.

Konečně polynom z příkladu ?? má reálný rozklad přibližně:

$p(x) \doteq 2\,(x-x_1)\,(x-x_2)\,(x-x_3)\,(x-x_4)\,(x^2+0{,}53872\,x+1{,}07814)\,(x^2-1{,}90584\,x+1{,}0499)$.

14.67. Příklad. Rozložíme polynom $x^5 - 10x^4 + 32x^3 - 8x^2 - 140x + 200$ na reálné kořenové činitele. Využijeme přitom nápovědy, že číslo $3 + i$ je kořenem tohoto polynomu.

Především je zřejmé, že se jedná o modelový příklad. Je totiž nereálné, aby nám v reálném životě někdo napovídal nereálný kořen reálného polynomu.

Protože má polynom reálné koeficienty, je podle věty ?? také číslo $3 - i$ kořenem. Známe tedy dva kořeny. Nyní máme dvě možnosti, jak dále postupovat. Můžeme například pomocí Hornerova schématu dosadit jednak $3 + i$ a následně $3 - i$ do polynomu. Druhou možností je roznásobit kořenové činitele příslušející známým kořenům a podělit výsledným kvadratickým polynomem daný polynom. Vyzkoušíme si obě metody.

Nejprve zkusíme dosazovat kořeny do Hornerova schématu. Zpočátku to půjde ztuha, protože člověk nenásobí dvě komplexní čísla mezi sebou denně.

	1	-10	32	-8	-140	200
$3+i$:		$3+i$	$-22-4i$	$34-2i$	$80+20i$	-200
	1	$-7+i$	$10-4i$	$26-2i$	$-60+20i$	0
$3-i$:		$3-i$	$-12+4i$	$-6+2i$	$60-20i$	
	1	-4	-2	20	0	

Ne náhodou máme na posledním řádku schématu reálná čísla. Tento řádek totiž obsahuje koeficienty polynomu r, pro který je $p(x) = (x-3-i)\,(x-3+i)\,r(x)$. Jak jsme ukázali v důkazu věty ??, polynom r má reálné koeficienty. Je tedy $p(x) = (x-3-i)\,(x-3+i)\,(x^3-4x^2-2x+20)$.

Než začneme rozkládat polynom r, zkusíme se ke stejnému mezivýsledku dostat druhou metodou. Roznásobíme nejdříve kořenové činitele $(x-3-i)\,(x-3+i) = x^2-6x+10$. Tím jsme se hned na začátku zbavili malého měkkého i. Abychom získali polynom r, musíme bohužel dělit polynom p polynomem $x^2-6x+10$.

$$
\begin{array}{rl}
(x^5-10x^4+32x^3-\ \ 8x^2-140x+200) & : (x^2-6x+10) = x^3-4x^2-2x+20 \\
-(x^5-\ \ 6x^4+10x^3) & \\
\hline
\quad -4x^4+22x^3-\ \ 8x^2-140x+200 & \\
\quad -(-4x^4+24x^3-40x^2) & \\
\hline
\qquad -2x^3+32x^2-140x+200 & \\
\qquad -(-2x^3+12x^2-\ \ 20x) & \\
\hline
\qquad\quad 20x^2-120x+200 & \\
\qquad\quad -(20x^2-120x+200) & \\
\hline
\qquad\qquad 0 &
\end{array}
$$

Ne náhodou vyšel zbytek po dělení nula. Polynom $x^2-6x+10$ musí dělit polynom p, protože se jedná o součin kořenových činitelů.

Nyní se nám obě metody setkávají. Potřebujeme rozložit polynom r na kořenové činitele. Hádáme mezi děliteli čísla 20: $r(1) = 15$ (není kořen), $r(-1) = 17$ (není kořen), $r(2) = 8$

(není kořen), $r(-2) = 0$ (ejhle kořen)! Po vydělení kořenovým činitelem $x+2$ (nebo použitím Hornerova schématu) dostáváme $r(x) = (x+2)\,(x^2-6+10)$. Protože polynom x^2-6+10 už v rozkladu jednou máme, shledáváme, že kořeny $3 \pm i$ jsou dvojnásobné. Reálný rozklad polynomu p tedy je

$$p(x) = (x+2)\,(x^2-6+10)^2.$$

14.68. Poznámka. V kalkulu jedné proměnné se studenti většinou seznamují se skutečností, že funkce dané podílem polynomů lze integrovat tak, že se tento podíl rozepíše na součet polynomu a parciálních zlomků. Přitom polynomy se integrují snadno a pro každý typ parciálního zlomku existuje integrační vzoreček.

Podlě věty ?? je možné funkci danou podílem polynomů částečně podělit. Platí $p/q = r + z/q$, přitom stupeň z je menší než stupeň q. Zlomek z/q je dále možno rozepsat na součet parciálních zlomků, jak uvidíme v následující větě ??. Nejprve ovšem potřebujeme dokázat pomocnou větu:

14.69. Věta. Nechť stupeň polynomu p je menší než stupeň polynomu q a nechť $\alpha \in \mathbf{C}$ je k-násobným kořenem polynomu q. Symbolem q_1 označme polynom, který splňuje $q(x) = (x-\alpha)^k q_1(x)$ pro všechna $x \in \mathbf{C}$. Pak existuje číslo $a \in \mathbf{C}$ a polynom p_1 tak, že platí

$$\frac{p(x)}{q(x)} = \frac{a}{(x-\alpha)^k} + \frac{p_1(x)}{(x-\alpha)^{k-1} q_1(x)}$$

pro všechna $x \in \mathbf{C}$ s výjimkou kořenů polynomu q. Přitom stupeň p_1 je menší než stupeň $(x-\alpha)^{k-1}q_1(x)$.

Důkaz. Vynásobením dokazované rovnosti polynomem q dostaneme ekvivalentní rovnost:

$$p(x) = a\,q_1(x) + p_1(x)\,(x-\alpha).$$

Dosazením $x = \alpha$ dostáváme $p(\alpha) = a\,q_1(\alpha)$, tedy $a = p(\alpha)/q_1(\alpha)$. Tento výpočet lze provést, protože díky větě ?? je $q_1(\alpha) \neq 0$.

Polynom $p(x) - a\,q_1(x)$ má kořen $\alpha \in \mathbf{C}$, protože $p(\alpha) - \big(p(\alpha)/q_1(\alpha)\big)\,q_1(\alpha) = 0$. Existuje tedy podle věty ?? polynom p_1 tak, že $p(x) - a\,q_1(x) = p_1(x)\,(x-\alpha)$. Přičtením $a\,q_1(x)$ a vydělením polynomem q dostáváme dokazovanou rovnost.

Protože $\mathrm{St}(p_1) + 1 \leq \max\big(\mathrm{St}(p), \mathrm{St}(q_1)\big) < \mathrm{St}(q)$, je $\mathrm{St}(p_1) < \mathrm{St}(q) - 1$. Takže platí i tvrzení o stupni polynomu p_1.

14.70. Věta. Nechť stupeň polynomu p je menší než stupeň polynomu q a nechť α je k-násobným kořenem polynomu q. Symbolem q_1 označme polynom, který splňuje $q(x) = (x-\alpha)^k q_1(x)$ pro všechna $x \in \mathbf{C}$. Pak existují čísla $a_1, a_2, \ldots, a_k \in \mathbf{C}$ a polynom p_2 tak, že platí:

$$\frac{p(x)}{q(x)} = \frac{a_k}{(x-\alpha)^k} + \frac{a_{k-1}}{(x-\alpha)^{k-1}} + \cdots + \frac{a_1}{(x-\alpha)} + \frac{p_2(x)}{q_1(x)}$$

pro všechna $x \in \mathbf{C}$ s výjimkou kořenů polynomu q. Přitom stupeň p_2 je menší než stupeň q_1.

Důkaz. Opakovaným použitím věty ??.

14.71. Věta. Podíl polynomů p/q, kde stupeň p je menší než stupeň q, je roven součtu konečně mnoha tzv. *parciálních zlomků* tvaru:

$$\frac{a}{(x-\alpha)^u}$$

kde $a \in \mathbf{C}$ je konstanta, $\alpha \in \mathbf{C}$ je kořen q násobnosti k a $u \leq k$, $u \in \mathbf{N}$.

Důkaz. Použijeme větu ?? postupně na všechny kořeny polynomu q.

14.72. Poznámka. Důkazy vět ?? a ?? jsou konstruktivní, tj. poskytují návod, jak spočítat konstanty, které se vyskytují v čitatelích všech parciálních zlomků. Čtenář by měl umět po pečlivém přečtení těchto důkazů implementovat algoritmus, který pro každé dva polynomy p a q (stupeň p je menší než stupeň q a u polynomu q jsou známy kořeny) sestaví součet parciálních zlomků.

V kurzech kalkulu jedné proměné se při integrování lomených funkcí (tj. funkcí ve tvaru podílu polynomů) pracuje s vybranými příklady, ve kterých se podaří najít kořeny jmenovatele. Je třeba si ale uvědomit, že pokud se nepodaří kořeny jmenovatele přesně najít (což je u polynomů stupně páteho a vyššího obvyklé), pak nelze přesně sestavit ani parciální zlomky a integrovat můžeme jen „teoreticky“.

14.73. Poznámka. Abychom se při integraci vyhnuli komplexním číslům, rozepisují se podíly polynomů s reálnými koeficienty na součet parciálních zlomků dvou druhů. Věta o součtu *reálných* parciálních zlomků má tvar:

14.74. Věta. Podíl polynomů p/q, kde stupeň p je menší než stupeň q a oba mají reálné koeficienty, je roven součtu konečně mnoha tzv. *parciálních zlomků* tvaru:

$$\frac{a}{(x-\alpha)^u} \quad \text{nebo} \quad \frac{bx+c}{(x^2+sx+t)^v},$$

kde $a \in \mathbf{R}$ je konstanta, $\alpha \in \mathbf{R}$ je kořen polynomu q násobnosti k a $u \leq k$, $u \in \mathbf{N}$. Dále $b, c \in \mathbf{R}$ jsou konstanty, kvadratický polynom (x^2+sx+t) má reálné koeficienty a je součinem $(x-\beta)\cdot(x-\overline{\beta})$, kde $\beta \in \mathbf{C}$, $\beta \notin \mathbf{R}$ je kořen polynomu q násobnosti r a platí $v \leq r$, $v \in \mathbf{N}$.

Důkaz. Ve větách ?? a ?? nahradíme všude množinu $\mathbf{C}$ množinou $\mathbf{R}$. Věty pak platí za předpokladu, že p a q jsou polynomy s reálnými koeficienty. K tomu musíme použít ještě následující větu:

14.75. Věta. Nechť p a q jsou polynomy s reálnými koeficienty a nechť stupeň p je menší než stupeň q. Předpokládejme, že $\beta \in \mathbf{C}$, $\beta \notin \mathbf{R}$ je k-násobným kořenem polynomu q. Symbolem

q_1 označme polynom, který splňuje $q(x) = (x-\beta)^k(x-\overline{\beta})^k q_1(x)$ pro všechna $x \in \mathbf{C}$. Pak existují čísla $b \in \mathbf{R}$, $c \in \mathbf{R}$ a polynom p_1 s reálnými koeficienty tak, že platí

$$\frac{p(x)}{q(x)} = \frac{bx+c}{(x-\beta)^k(x-\overline{\beta})^k} + \frac{p_1(x)}{(x-\beta)^{k-1}(x-\overline{\beta})^{k-1}q_1(x)}$$

pro všechna $x \in \mathbf{C}$ s výjimkou kořenů polynomu q. Přitom stupeň polynomu p_1 je menší než stupeň $(x-\beta)^{k-1}(x-\overline{\beta})^{k-1}q_1(x)$.

Důkaz. Vynásobením dokazované rovnosti polynomem q dostaneme ekvivalentní rovnost:

$$p(x) = (bx+c)\,q_1(x) + p_1(x)\,(x-\beta)\,(x-\overline{\beta}).$$

Dosazením $x = \beta$ dostáváme $p(\beta) = (b\,\beta + c)\,q_1(\beta)$. Musí tedy platit $b\,\beta + c = p(\beta)/q_1(\beta)$. Tento výpočet lze provést, protože díky větám ?? a ?? je $q_1(\beta) \neq 0$.

Označme $\beta = u + iv$ a $p(\beta)/q_1(\beta) = t + is$, kde $u, v, t, s \in \mathbf{R}$. Je $b\,(u+iv) + c = t + is$, takže $b = s/v$ a $c = t - (s/v)\,u$. Z výpočtu plyne, že čísla b, c existují a jsou reálná.

Polynom $p(x) - (bx+c)\,q_1(x)$ má kořen $\beta \in \mathbf{C}$, protože $p(\beta) - \big(p(\beta)/q_1(\beta)\big)\,q_1(\beta) = 0$. Tento polynom má také kořen $\overline{\beta}$, protože má reálné koeficienty a platí věta ??. Existuje tedy podle věty ?? polynom p_1 s reálnými koeficienty tak, že $p(x) - (bx+c)\,q_1(x) = p_1(x)\,(x-\beta)(x-\overline{\beta})$. Přičtením $(bx+c)\,q_1(x)$ a vydělením polynomem q dostáváme dokazovanou rovnost.

Protože $\mathrm{St}(p_1) + 2 \leq \max\big(\mathrm{St}(p), \mathrm{St}(q_1)+1\big) < \mathrm{St}(q)$, je $\mathrm{St}(p_1) < \mathrm{St}(q) - 2$. Takže platí i tvrzení o stupni polynomu p_1.

14.76. Poznámka. Ukázkové příklady na převod lomené funkce na součet parciálních zlomků najde čtenář v mnoha jiných učebních textech ke kalkulu. Nebo může použít matematický software, který zvládá rozpis na součet parciálních zlomků. Nás zde hlavně zajímalo zdůvodění vyslovených vět.

14.77. Definice. Nechť polynom p má koeficienty z nějakého tělesa T. Pokud vyhodnocujeme polynom jen pro $x \in T$ a operace $+, \cdot$ ve vzorci pro hodnotu polynomu jsou operace definované v tělese T, pak říkáme, že polynom p je *nad tělesem T*.

Nechť p je polynom nad tělesem T. Říkáme, že *p je reducibilní v T*, pokud existují polynomy q, r stupně aspoň prvního nad T tak, že $p = q\,r$. Polynom p je *ireducibilní v T*, jestliže není reducibilní v T.

14.78. Poznámka. Slovo *ireducibilní* můžeme přeložit jako *nerozložitelný* na součin polynomů nižšího stupně v číselném oboru koeficientů, který je stanoven tělesem T. Například polynom $x^2 + 1$ je ireducibilní v $\mathbf{R}$, ale není ireducibilní v $\mathbf{C}$, protože $x^2 + 1 = (x - i)(x + i)$.

Z definice je zřejmé, že konstantní polynomy a polynomy stupně prvního jsou určitě ireducibilní v libovolném tělese, protože podle věty ?? nemohou existovat dva polynomy stupně aspoň prvního, jejichž součin je polynom stupně nejvýše prvního.

Z fundamentální věty algebry plyne tento důležitý poznatek: *ireducibilní polynomy v $\mathbf{C}$ jsou pouze polynomy stupně nejvýše prvního*, nebo jinak: *všechny polynomy stupně aspoň*

druhého jsou v $\mathbf{C}$ *reducibilní*, nebo ještě jinak: *pro každý nenulový polynom existuje rozklad na kořenové činitele, což je rozklad na součin ireducibilních polynomů v* $\mathbf{C}$.

Reálný rozklad popsaný ve větě ?? je rozkladem na součin ireducibilních polynomů v $\mathbf{R}$. Z této věty plyne, že *ireducibilní polynom v* $\mathbf{R}$ *má stupeň nejvýše* 2. Ireducibilní polynom $ax^2 + bx + c$ v $\mathbf{R}$ stupně druhého poznáme tak, že má záporný diskriminant $D = b^2 - 4ac$.

Má-li polynom stupně aspoň druhého nad tělesem T kořen v tělese T, pak je reducibilní v T. Obrácené tvrzení „nemá-li polynom v tělese T kořen, pak je ireducibilní v T“ neplatí. Například $(x^2+1)^2$ nemá v $\mathbf{R}$ kořen, ale lze jej rozložit na součin polynomů $(x^2+1)(x^2+1)$ s reálnými koeficienty.

14.79. Příklad. Polynom $x^8 - 1$ z příkladu ?? má rozklad na součin ireducibilních polynomů v $\mathbf{C}$:

$$x^8-1 = \left(x-1\right)\left(x-\tfrac{\sqrt2}{2}-i\tfrac{\sqrt2}{2}\right)\left(x-\tfrac{\sqrt2}{2}+i\tfrac{\sqrt2}{2}\right)\left(x-i\right)\left(x+i\right)\left(x+\tfrac{\sqrt2}{2}-i\tfrac{\sqrt2}{2}\right)\left(x+\tfrac{\sqrt2}{2}+i\tfrac{\sqrt2}{2}\right)\left(x+1\right),$$

zatímco rozklad téhož polynomu na součin ireducibilních polynomů v $\mathbf{R}$ je

$$x^8 - 1 = (x-1)(x+1)(x^2+1)(x^2+\sqrt2\,x+1)(x^2-\sqrt2\,x+1)$$

a konečně rozklad na součin ireducibilních polynomů v $\mathbf{Q}$ (tělese racionálních čísel) vypadá následovně:

$$x^8 - 1 = (x-1)(x+1)(x^2+1)(x^4+1).$$

14.80. Shrnutí. Polynom jsme zavedli jako funkci danou vzorečkem /??/ nebo jako vzoreček samotný /??/. Definovali jsme součet a skalární násobek těchto vzorečků /??/ a ukázali, že tvoří lineární prostor /??/, který je izomorfní s prostorem polynomů jako funkcí /??/.

Kromě sčítání polynomů a násobení polynomu konstantou umíme polynomy také násobit mezi sebou /??/ a hledat částečný podíl /??/.

Uvedli jsme si /??/, že Hornerovo schéma umožní nejen efektivně vyhodnocovat polynomy ve zvolených bodech α, ale mezivýpočty navíc tvoří koeficienty částečného podílu vyhodnocovaného polynomu polynomem $(x - \alpha)$.

Definovali jsme kořen polynomu /??/ a dokázali, že polynom je dělitelný svým kořenovým činitelem beze zbytku /??/. Z toho vyplynul rozklad polynomu na součin kořenových činitelů /??/. Základní věta algebry /??/ zaručuje, že tento rozklad lze provést v oboru komplexních čísel. Přitom si musíme být vědomi, že pro obecné polynomy stupně pátého a vyššího vzorce na přesný výpočet kořenů z koeficinetů neexistují /??/, takže rozklad je možné psát jen teoreticky.

Uvedli jsme si věty /??, ??/, které uvádějí, že v případě celočíselných koeficientů dělí případné celočíselné kořeny koeficient a_0 resp. případný racionální kořen má jistý vztah ke koeficientům a_0 a a_n. Ovšem problém je v tom, že polynom s celočíselnými koeficienty nemusí mít žádný racionální kořen (což je navíc typická vlastnost). Pomůže nám to ke hledání kořenů jen pro „modelové příklady“.

Věty /??, ??/ říkají, že polynomy s reálnými koeficienty mají své nereálné komplexní kořeny v párech vzájemně komplexně sdružené a stejné násobnosti. To inspiruje k reálnému

rozkladu polynomu na součin: stačí snásobit kořenové činitele typu $(x-\alpha)(x-\overline{\alpha})$, což je kvadratický polynom s reálnými koeficienty a se záporným diskriminantem.

Krátce jsme zmínili rozklad racionální lomené funkce na parciální zlomky /??, ??/ včetně reálné alternativy /??, ??/.

Definovali jsme pojem ireducibilní polynom /??/.

15. Grupa, těleso

15.1. Poznámka. Následující text až do konce kapitoly je poněkud abstraknější povahy. Přitom se jeho znalost nepředpokládá pro pochopení dalších kapitol. Pokud tedy čtenář nechce být hned v počátku studia zahlcen pojmy o algebraických strukturách, může tento text přeskočit.

15.2. Poznámka. Reálná čísla jsou množina prvků, které umíme vzájemně sčítat a vzájemně násobit. Přesněji, je to množina $\mathbf{R}$, na které jsou definovány obvyklé operace $+ \colon \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ a $\cdot \colon \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ s jistými vlastnostmi (asociativní zákon, distributivní zákon, atd.). Těmito vlastnostmi se budeme inspirovat a pokusíme se vybudovat abstraktní algebraickou strukturu, tzv. *těleso*. Jedním z možných konkrétních příkladů tělesa pak samozřejmě budou reálná čísla. Jenomže kromě nich budeme nacházet i jiné příklady těles. Začneme nejprve strukturou s jedinou operací.

15.3. Definice. Množinu G, na které je definována operace $\circ : G \times G \to G$ nazýváme *grupou*, pokud pro tuto operaci platí:

(1) $\forall x, y, z \in G : (x \circ y) \circ z = x \circ (y \circ z)$ (asociativní zákon),

(2) $\exists e \in G$, pro které platí $\forall x \in G : e \circ x = x \circ e = x$ (existence neutrálního/jednotkového

(3) $\forall x \in G\ \exists y \in G : x \circ y = y \circ x = e$ (existence opačného/inverzního prvku y pro každý pr

Pokud navíc platí

(4) $\forall x, y \in G : x \circ y = y \circ x$ (komutativní zákon),

pak grupu G nazýváme *komutativní grupou*. Z historických důvodů a z úcty k norskému matematikovi, který rozpracoval teorii grup a bohužel zemřel mlád na zákeřnou nemoc ve věku 26 let, se komutativní grupa nazývá též *Abelova grupa*.

15.4. Poznámka. Niels Abel mimo jiné pomocí teorie grup dokázal, že nelze pro obecný polynom stupně vyššího než 4 najít vzorec na výpočet jeho kořenů z jeho koeficientů. Pro polynomy stupně 1, 2, 3 a 4 přitom takové vzorce existují. Pro stupeň 2 se jej žáci učí zpaměti: $x_{1,2} = (-b \pm \sqrt{b^2 - 4ac})/2a$.

15.5. Příklad. Jednoprvková množina $G = \{e\}$ s operací $e \circ e = e$ je nejmenší možnou grupou.

15.6. Příklad. Množina $\mathbf{R}$ s operací sčítání tvoří grupu. Skutečně platí asociativní zákon pro sčítání reálných čísel: $(x + y) + z = x + (y + z)$, dále existuje neutrální prvek 0, pro který $0 + x = x + 0 = x$ a konečně pro každé $x \in \mathbf{R}$ existuje $y = -x$ tak, že $x + y = y + x = 0$. Navíc se jedná o grupu komutativní, protože sčítání reálných čísel je komutativní.

Pokud operaci grupy značíme symbolem „+“ (jako v tomto příkladě), pak obvykle o prvku e z vlastnosti (2) mluvíme jako o neutrálním prvku a značíme ho symbolem „0“ (též nula, nulový prvek) a prvek y z vlastnosti (3) nazýváme *opačný* a značíme $-x$. Přičtení opačného prvku v komutativní grupě pak nazýváme *odečítání* a místo $a + (-b)$ píšeme $a - b$.

15.7. Příklad. Množina $\mathbf{R} \setminus \{0\}$ s operací násobení tvoří grupu. Skutečně platí asociativní zákon pro násobení reálných čísel: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, dále existuje jednotkový prvek 1, pro který $1 \cdot x = x \cdot 1 = x$ a konečně pro každé $x \in \mathbf{R} \setminus \{0\}$ existuje $y = x^{-1}$ tak, že $x \cdot y = y \cdot x = 1$. Navíc se jedná o grupu komutativní, protože násobení reálných čísel je komutativní.

Pokud operaci grupy značíme symbolem „$\cdot$“, pak obvykle prvek e z vlastnosti (2) značíme symbolem „1“ (jedna, jednotkový prvek). Prvek y z vlastnosti (3) nazýváme *inverzní* a značíme x^{-1}. Násobení inverzním prvkem v komutativní grupě nazýváme *dělení* a místo $a \cdot b^{-1}$ píšeme a/b nebo $\frac{a}{b}$.

15.8. Příklad. Množina $\mathbf{R}$ s operací násobení netvoří grupu, protože 0 nemá inverzní prvek.

15.9. Příklad. Množina všech reálných funkcí $F = \{f : \mathbf{R} \to \mathbf{R},\ f$ je prostá a „na“$\}$ s operací *skládání funkcí* $\circ\colon F \times F \to F$, definovanou pomocí $(g \circ f)(x) = g\big(f(x)\big)\ \forall x \in \mathbf{R}$, tvoří grupu. Skutečně platí asociativní zákon $(f \circ g) \circ h = f \circ (g \circ h)$ a existuje jednotkový prvek: identické zobrazení i, pro které $i(x) = x$. Ke každé prosté funkci f lze setrojit funkci inverzní f^{-1} tak, že $f \circ f^{-1} = f^{-1} \circ f = i$. Přitom se nejedná o grupu komutativní, protože například pro $f(x) = x^3$, $g(x) = 1 + x$ je $(f \circ g)(x) = (1 + x)^3$, zatímco $(g \circ f)(x) = 1 + x^3$.

15.10. Příklad. Kdybychom v předchozím příkladě místo funkcí f z $\mathbf{R}$ na $\mathbf{R}$ uvažovali prostá zobrazení p z nějaké množiny M na M, dostáváme znovu grupu, která nemusí být komutativní. V případě konečné množiny M se jedná o grupu permutací.

15.11. Příklad. Množina $M \subseteq \mathbf{R}^{n,n}$ všech regulárních matic (viz ??) s operací násobení matic tvoří příklad nekomutativní grupy.

15.12. Příklad. Množina čísel $\{0, 1, 2, \ldots, k-1\}$ s operací $a \oplus b = a + b$ modulo k tvoří komutativní grupu. Připomínáme, že „x modulo y“ je zbytek při dělení čísla x číslem y. Neutrálním prvkem této grupy je 0 a opačným prvkem k prvku $a \neq 0$ je prvek $k - a$. Samozřejmě, opačným prvkem k prvku neutrálnímu je prvek neutrální, což ostatně platí v libovolné grupě.

15.13. Příklad. Lineární prostor se svou operací sčítání vektorů (podle definice ??) tvoří komutativní grupu. Skutečně, asociativní zákon je postulován vlastností (2) v definici ??,

neutrálním prvkem je nulový vektor (viz vlastnost (1) věty ??) a opačný vektor k vektoru $\boldsymbol{x}$ je vektor $-\boldsymbol{x} = (-1)\cdot\boldsymbol{x}$, protože

$$(-1)\cdot\boldsymbol{x} + \boldsymbol{x} = (-1)\cdot\boldsymbol{x} + 1\cdot\boldsymbol{x} = (-1+1)\cdot\boldsymbol{x} = 0\cdot\boldsymbol{x} = \boldsymbol{o}.$$

Konečně z vlastnosti (1) definice ?? plyne, že se jedná o grupu komutativní.

15.14. Poznámka. Obráceně, pomocí pojmu grupa můžeme významně zkrátit naší definici lineárního prostoru ??:

Lineárním prostorem je množina L, která s operací $+\colon L\times L\to L$ tvoří komutativní grupu. Dále musí být na množině L definována operace $\cdot\colon \mathbf{R}\times L\to L$, s vlastnostmi $\forall\alpha,\beta\in\mathbf{R}, \forall\boldsymbol{x},\boldsymbol{y}\in L$:

$$\begin{aligned}
&\text{(A)} \quad \alpha\cdot(\beta\cdot\boldsymbol{x}) = (\alpha\beta)\cdot\boldsymbol{x},\\
&\text{(B)} \quad \alpha\cdot(\boldsymbol{x}+\boldsymbol{y}) = \alpha\cdot\boldsymbol{x} + \alpha\cdot\boldsymbol{y},\\
&\text{(C)} \quad (\alpha+\beta)\cdot\boldsymbol{x} = \alpha\cdot\boldsymbol{x} + \beta\cdot\boldsymbol{x},\\
&\text{(D)} \quad 1\cdot\boldsymbol{x} = \boldsymbol{x}.
\end{aligned}$$

Vzhledem k tomu, že vlastnosti (1), (2) definice ?? přímo korespondují s vlastnostmi komutativní grupy, stačí ověřit, že nám z této nové definice vyplyne vlastnost (7) definice ??, která jediná zde chybí. Existence nulového vektoru je zajištěna jako existence neutrálního prvku $\boldsymbol{o}$ v grupě. Je potřeba ukázat, že pro libovolný $\boldsymbol{x}\in L$ je vektor $0\cdot\boldsymbol{x}$ roven neutrálnímu

prvku $\boldsymbol{o}$. K vektoru $0 \cdot \boldsymbol{x}$ ovšem existuje v grupě prvek opačný $-0 \cdot \boldsymbol{x}$. Ten přičteme k oběma stranám rovnice $0 \cdot \boldsymbol{x} = (0+0) \cdot \boldsymbol{x} = 0 \cdot \boldsymbol{x} + 0 \cdot \boldsymbol{x}$. Na levé straně dostáváme $0 \cdot \boldsymbol{x} + (-0 \cdot \boldsymbol{x}) = \boldsymbol{o}$. Na pravé straně je $0 \cdot \boldsymbol{x} + 0 \cdot \boldsymbol{x} + (-0 \cdot \boldsymbol{x}) = 0 \cdot \boldsymbol{x} + \boldsymbol{o} = 0 \cdot \boldsymbol{x}$. Porovnáním levé a pravé strany máme výsledek $\boldsymbol{o} = 0 \cdot \boldsymbol{x}$.

15.15. Poznámka. Axiomy grupy v definici ?? explicitně neuvádějí, že v grupě existuje jen jediný neutrální prvek a ke každému prvku existuje jen jediný prvek opačný. Následující věta ukazuje, že to nicméně platí jako jednoduchý důsledek axiomů.

15.16. Věta. (A) Každá grupa má jen jediný neutrální/jednotkový prvek. (B) Ke každému prvku grupy existuje jediný opačný/inverzní prvek.

Důkaz. (A) Předpokládáme dva neutrální prvky e_1, e_2. Musí platit $e_1 = e_1 \circ e_2$, protože e_2 je neutrální. Musí také platit $e_2 = e_1 \circ e_2$, protože e_1 je neutrální. Takže $e_1 = e_1 \circ e_2 = e_2$ a neutrální prvky se neliší.

(B) Nechť $x \in G$ má dva inverzní/opačné prvky y_1 a y_2. Označme e neutrální prvek. Pak platí: $y_1 = e \circ y_1 = (y_2 \circ x) \circ y_1 = y_2 \circ (x \circ y_1) = y_2 \circ e = y_2$, takže $y_1 = y_2$.

15.17. Věta. Nechť na neprázdné množině G je dána operace $\circ : G \times G \to G$, pro kterou platí asociativní zákon (1) z definice grupy ??. Pak vlastnosti (2) a (3) z definice grupy jsou

ekvivalentní s vlastností: pro každé $a, b \in G$ existují $x, y \in G$, které řeší rovnice $a \circ x = b$ a $y \circ a = b$.

Důkaz. Nechť nejprve platí vlastnosti (1), (2), (3) z definice grupy ??. Označme a^{-1} inverzní prvek k prvku a. Pak $x = a^{-1} \circ b$ řeší rovnici $a \circ x = b$, protože $a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b$. Z podobných důvodů $y = b \circ a^{-1}$ řeší rovnici $y \circ a = b$.

Nechť nyní platí asociativní zákon (1) a umíme řešit uvedené rovnice. Volme $a \in G$. Označme e_a řešení rovnice $a \circ x = a$, tj. platí $a \circ e_a = a$. Ukážeme nejprve, že pro libovolné $b \in G$ je $b \circ e_a = b$. Nechť $y \in G$ řeší rovnici $y \circ a = b$. Pak platí $b \circ e_a = (y \circ a) \circ e_a = y \circ (a \circ e_a) = y \circ a = b$. Vidíme tedy, že řešení e_a rovnice $a \circ x = a$ nezávisí na volbě prvku a, takže stačí prvek e_a označovat e. Podobně lze ukázat, že také řešení rovnice $y \circ a = a$ nezávisí na volbě prvku a. Označme toto řešení f. Nyní podobně jako v důkazu věty ?? je $f \circ e = f$, protože e řeší $a \circ e = a$ a platí $f \circ e = e$, protože f řeší $f \circ a = a$. Takže $e = f$ a toto je jednotkový prvek grupy.

Sestrojíme inverzní prvek k prvku $x \in G$. Nechť u řeší rovnici $x \circ u = e$ a v řeší rovnici $v \circ x = e$. Platí $v = v \circ e = v \circ (x \circ u) = (v \circ x) \circ u = e \circ u = u$, takže $u = v$ je inverzní prvek k prvku x.

15.18. Poznámka. Vzhledem k předchozí větě se v některé literatuře definuje grupa jen pomocí asociativního zákona a řešitelnosti rovnic (jen dvě vlastnosti). Pokud platí jen asociativní zákon a řešitelnost rovnic není požadována, mluví se o *pologrupě*. Pokud je pouze dána

operace $\circ : G \times G \to G$ bez dalších vlastností, mluví se v některé literatuře o *grupoidu*. Takže množina s operací je grupoid. Grupoid s asociativním zákonem je pologrupa. Pologrupa s řešitelností rovnic je grupa.

15.19. Definice. Nechť G je grupa s operací $\circ$. Pokud $G_1 \subset G$ je sama o sobě grupou se stejnou operací (tj. speciálně $\circ : G_1 \times G_1 \to G_1$ a platí vlastnosti (1)–(3) definice grupy ??), nazýváme G_1 *podgrupou* grupy G.

15.20. Poznámka. Výše uvedenou definici uvádím hlavně proto, aby měl čtenář možnost ji porovnat s definicí podprostoru ?? a shledal, že základní myšlenka definice podstruktury je pořád stejná. V případě ověřování podgrupy je kontrola asociativního zákona (1) zbytečná (je zaručen už ve vnější grupě), ale vlastnosti $x \circ y \in G_1$, $e \in G_1$ a existence inverzního prvku v G_1 jsou podstatné.

15.21. Příklad. Množina $\mathbf{Z}$ celých čísel s operací sčítání „+“ je podgrupou grupy $\mathbf{R}$ reálných čísel se stejnou operací.

15.22. Příklad. Množina $\mathbf{Z} \setminus \{0\}$ celých nenulových čísel s operací násobení „$\cdot$“ není podgrupou grupy $\mathbf{R} \setminus \{0\}$ reálných čísel se stejnou operací, protože k číslům různým od -1 a 1 neexistuje na množině $\mathbf{Z} \setminus \{0\}$ inverzní prvek. Na druhé straně se jedná o pologrupu, protože násobení je uzavřeno na nenulová celá čísla a je samozřejmě asociativní.

15.23. Definice. *Těleso* je množina T se dvěma operacemi obvykle označovanými $+ : T \times T \to T$ a $\cdot : T \times T \to T$, které mají následující vlastnosti:

(1) T s operací „+“ je komutativní grupa. Neutrální prvek této grupy je označen symbolem 0.

(2) $T \setminus \{0\}$ s operací „$\cdot$“ je komutativní grupa. Jednotkový prvek této grupy se značí symbolem 1.

(3) Operace „+“ a „$\cdot$“ splňují distributivní zákon: $a \cdot (b + c) = a \cdot b + a \cdot c$.

15.24. Poznámka. Někteří autoři v definici tělesa nepožadují komutativitu grupy vzhledem k násobení a pokud je splněna, mluví o *komutativním tělese*. Existují příklady, kdy komutativita násobení není splněna Důležitým příkladem jsou *kvaterniony*: čísla podobná komplexním, ale se třemi nezávislými imaginárními jednotkami. Kvaterniony se užívají například při popisu 3D transformací v počítačové grafice [28]. V našem textu budeme u těles vždy předpokládat komutativitu obou operací.

15.25. Příklad. Reálná čísla s operacemi sčítání a násobení tvoří těleso.

15.26. Příklad. Racionální čísla jsou podtělesem tělesa reálných čísel. Podtěleso je definováno v souladu s poznámkou ?? jako podmnožina tělesa, která sama o sobě se stejnými operacemi tvoří těleso.

15.27. Příklad. Množina celých čísel s operacemi sčítání a násobení netvoří těleso, protože pro operaci násobení neexistuje pro všechna nenulová celá čísla inverzní prvek jako celé číslo. Toto je příklad struktury, která má všechny vlastnosti tělesa s výjimkou jediné: není zaručena existence inverzního prvku pro násobení. Taková struktura se nazývá *okruh*.

15.28. Příklad. Množina komplexních čísel s operacemi sčítání a násobení tvoří těleso.

15.29. Věta. Pro libovolné prvky a, b z tělesa platí: $a \cdot b = 0$ právě tehdy, když $a = 0$ nebo $b = 0$.

Důkaz. ($\Rightarrow$): $T \setminus \{0\}$ musí být podle vlastnosti (2) definice ?? vzhledem k násobení grupa, tj. součin dvou nenulových prvků musí být prvek nenulový. Jinými slovy, pokud součin vychází nulový, musí aspoň jeden z činitelů být nula.

($\Leftarrow$): Je třeba dokázat, že $0 \cdot a = 0$. Protože 0 je neutrální prvek vzhledem ke sčítání, platí $0 + 0 = 0$. Díky distributivnímu zákonu je $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$. K oběma stranám rovnosti přičteme opačný prvek k prvku $0 \cdot a$, tedy prvek $-0 \cdot a$. Na levé straně dostáváme 0 a na pravé $0 \cdot a$.

15.30. Příklad. Těleso musí podle definice obsahovat 0 a 1 a tyto dva prvky musejí být různé. Takže těleso musí obsahovat aspoň dva prvky. Ukážeme, že existuje těleso, které obsahuje jen tyto dva prvky, tedy $T = \{0, 1\}$.

Operaci „+“ definujeme: $0+0=0,\ 0+1=1+0=1,\ 1+1=0$. Operaci „$\cdot$“ definujeme jako obvyklé násobení: $0\cdot 0=0\cdot 1=1\cdot 0=0,\ 1\cdot 1=1$. Množina $T=\{0,1\}$ s takto zavedenými operacemi tvoří těleso.

Skutečně, pro operaci „+“ platí asociativní zákon, 0 je neutrální prvek, opačný prvek k 0 je 0 a opačný prvek k 1 je 1. Grupa $T\setminus\{0\}$ vzhledem k násobení je jednoprvková a všechny vlastnosti grupy zde platí zcela samozřejmě. Je rovněž splněn distributivní zákon.

Sčítání je v tomto tělese totéž co odečítání. Inverzní prvek k 1 je 1.

Tělesa s konečně mnoha prvky se z historických důvodů nazývají *Galoisova tělesa*. V našem příkladě $T=\{0,1\}$ se tedy jedná o Galoisovo těleso se dvěma prvky.

Évariste Galois byl francouzský matematik, který bohužel zemřel mlád ve věku 20 let na následky zranění v souboji. I jeho teorie dokazuje mimo jiné nemožnost algebraického popisu kořenů polynomů stupně většího než 4. Tato teorie je známější než Abelova, ovšem byla zveřejněna o pět let později.

15.31. Poznámka. Je-li třeba na dvouprvkové množině definovat operace sčítání a násobení tak, abychom získali těleso, není možné to udělat jinak, než v příkladu ??. Především 0 je neutrální prvek vzhledem ke sčítání, takže podle vlastnosti (2) definice grupy ?? musí $0+0=0$, $0+1=1+0=1$. Dále množina $\{1\}$ musí být grupou vzhledem k násobení, takže musí $1\cdot 1=1$. Dále musí platit $0\cdot a=a\cdot 0=0$, jinak by nebyla splněna věta ??. Zbývá otázka, zda můžeme definovat $1+1=1$. Nemůžeme, protože pak by prvek 1 neměl prvek opačný.

15.32. Příklad. Na množině $\{0, 1, \ldots, p-1\}$ definujme operace „+“ a „·“ jako obvyklé sčítání a násobení, ovšem na výsledek aplikujme proces „modulo p“. Takže například pro $p = 5$ pracujeme s množinou $\{0, 1, 2, 3, 4\}$ a platí $4 + 3 = 2$, protože zbytek po dělení čísla 7 číslem 5 je 2. Nebo $4 \cdot 4 = 1$, protože zbytek po dělení čísla 16 číslem 5 je 1.

Nechť nejprve p není prvočíslo, tj. je tvaru součinu $p = m\,n$. Pak $m \cdot n = 0$ modulo p, a přitom čísla m a n jsou nenulová. Podle věty ?? se nemůže jednat o těleso, protože součin nenulových čísel musí v tělese vyjít jako číslo nenulové.

Nechť p je prvočíslo. Ukážeme, že $M = \{0, 1, \ldots, p-1\}$ s operacemi „+, · modulo p“ tvoří těleso. Především M se sčítáním modulo p je komutativní grupa (viz příklad ??). Operace násobení modulo p je asociativní, komutativní a jednotkovým prvkem je číslo 1. Distributivní zákon plyne z distributivního zákona běžných operací „+“ a „·“. Nejvíce práce dá nalezení inverzního prvku pro $a \in M \setminus \{0\}$. Prvek a nechme pevný a uvažujme všechna čísla „ak modulo p“ pro $k \in \{1, 2, \ldots, p-1\}$. Tato čísla jsou pro různá k vzájemně různá (viz níže) a pokrývají tedy celou množinu $\{1, 2, \ldots, p-1\}$. Musí tedy existovat takové k, že $ak = 1 \bmod p$. Toto k je inverzním prvkem k prvku a. V úvaze ještě chybí obhájit, že čísla „ak modulo p“ jsou pro různá k vzájemně různá. Předpokládejme, že existují čísla $k_1, k_2 \in M \setminus \{0\}$, $k_1 \geq k_2$ taková, že $ak_1 = ak_2 \bmod p$, tj. $a(k_1 - k_2) = mp$ pro nějaké $m \geq 0$. Rovnost vydělíme číslem a. Protože $a < p$ a p je prvočíslo, existuje $m_1 \geq 0$, že po vydělení číslem a dostáváme $k_1 - k_2 = m_1 p$. Vlevo je číslo menší než p, takže musí být $m_1 = 0$, tj. $k_1 = k_2$.

Podle počtu prvků p se toto těleso označuje $\mathrm{GF}(p)$. Jiné značení $\mathbf{Z}_p$ dává najevo, že se jedná o celá čísla „modulo p“. Předchozí příklad ?? definuje konečné těleso $\mathbf{Z}_p$ pro $p = 2$.

15.33. Definice. *Charakteristika tělesa* udává nejmenší kladný počet jedniček, jejichž součet dává nulu. Tedy pokud je $\sum_1^\lambda 1 = 0$ a λ je nejmenší kladné číslo s touto vlastností, pak těleso má charakteristiku λ. Pokud tato vlastnost není splněna pro žádný počet jedniček, je charakteristika rovna ∞.

15.34. Příklad. Charakteristika tělesa reálných čísel je ∞. Charakteristika tělesa $\mathbf{Z}_p$ je p.

15.35. Věta. Charakteristika tělesa je nekonečná nebo to je prvočíslo.

Důkaz. Sporem. Nechť pro charakteristiku λ platí $\lambda = mn$, $m \neq \lambda$, $n \neq \lambda$. Z distributivního zákona plyne $(\sum_1^m 1) \cdot (\sum_1^n 1) = \sum_1^{mn} 1 = \sum_1^\lambda 1 = 0$. Podle věty ?? musí být aspoň jedna suma v závorce rovna nule, protože jejich součin je nulový. To je spor s tím, že λ je nejmenší počet jedniček, jejichž součet je nulový.

15.36. Poznámka. Kromě $\mathrm{GF}(p)$, kde p je prvočíslo, existují konečná tělesa s počtem prvků p^m, kde p je prvočíslo, m je libovolná mocnina, značení: $\mathrm{GF}(p^m)$. Jak jsme ukázali v příkladě ??, konstrukce operací pro $\mathrm{GF}(p^m)$ nemůže vycházet jen z myšlenky „modulo p“. Ve skutečnosti je konstrukce tělesa $\mathrm{GF}(p^m)$ výrazně komplikovanější. V následujícím příkladě je pro ilustraci popsáno těleso $\mathrm{GF}(2^3)$.

Z věty ?? plyne, že i tělesa $\mathrm{GF}(p^m)$ musejí mít charakteristiku ve tvaru prvočísla. Kdybychom zde měli prostor na podrobnější popis těles $\mathrm{GF}(p^m)$, shledali bychom, že mají charakteristiku p.

Dá se dále ukázat, že pokud má mít těleso konečný počet prvků, pak tento počet nemůže být jiný než p^m, kde p je prvočíslo a m přirozené číslo. Navíc operace na konečném tělese lze definovat jediným možným způsobem (lišit se může jen způsob označení prvků).

15.37. Příklad. Uvažujme množinu všech uspořádaných trojic prvků ze $\mathbf{Z}_2$ indexovaných čísly. Nulová trojice nemá žádný index a ostatní trojice mají přiřazeny indexy 0 až 6:

$$\{(0,0,0)_*,\ (1,0,0)_0,\ (0,1,0)_1,\ (0,0,1)_2,\ (1,1,0)_3,\ (0,1,1)_4,\ (1,1,1)_5,\ (1,0,1)_6\}.$$

Prvky této množiny budeme sčítat tak, že si indexů nebudeme všímat a budeme sčítat jen uspořádané trojice v aritmetice $\mathbf{Z}_2$. Například $(1,1,0)_3 + (0,1,1)_4 = (1,0,1)_6$, protože je $(1,1,0) + (0,1,1) = (1,0,1)$ v aritmetice $\mathbf{Z}_2$.

Výsledek násobení kteréhokoli prvku s prvkem $(0,0,0)_*$ definujeme jako $(0,0,0)_*$. Jedná se o nulový prvek tělesa. Násobení nenulových prvků definujeme tak, že si nevšímáme uspořádaných trojic, ale jen indexů. Ty sečteme a provedeme operaci modulo 7. Například $(0,1,1)_4 \cdot (1,1,1)_5 = (0,0,1)_2$, protože $4 + 5$ modulo $7 = 2$. Dá se ukázat, že tento příklad splňuje axiomy tělesa. Obsahuje 2^3 prvků, takže se jedná o příklad tělesa $\mathrm{GF}(2^3)$.

Jak již bylo řečeno, je $(0,0,0)_*$ nulový prvek. Rovněž je zřejmé, že $(1,0,0)_0$ je jednotkový prvek tohoto tělesa. Inverzní prvek například k $(0,0,1)_2$ je $(1,1,1)_5$, protože $2 + 5$ modulo $7 = 0$. Opačný prvek k libovolnému prvku x je prvek x, protože v aritmetice $\mathbf{Z}_2$ je $1 + 1 = 0$. Charakteristika tohoto tělesa je 2.

Prosím čtenáře, aby se nesnažil hrubou silou ověřit platnost distributivního zákona tohoto tělesa (jde to, ale není to příliš účelné) ani příliš nehloubal nad tím, proč například trojice $(1,1,1)$ má index 5. Pro odpovědi na tyto otázky je potřeba použít vlastnosti ireducibilních polynomů nad tělesem $\mathbf{Z}_2$ (obecně nad tělesem $\mathbf{Z}_p$), což bohužel překračuje rámec tohoto úvodního textu.

15.38. Poznámka. V definici lineárního prostoru ?? jsme sice byli dostatečně abstraktní (vektory, ani operace s nimi jsme blíže nespecifikovali), ale pracovali jsme tam s docela konkrétní množinou $\mathbf{R}$ reálných čísel. Pokud v této definici nahradíme množinu $\mathbf{R}$ pojmem těleso (s blíže nespecifikovanými prvky a operacemi), dostáváme lineární prostor nad tělesem. Můžeme pak pracovat s lineárním prostorem nad tělesem komplexních čísel, lineárním prostorem nad tělesem $\mathbf{Z}_2$ atd.

Pokusíme se tedy do třetice přepsat definici lineárního prostoru, tentokrát nad libovolným tělesem.

15.39. Definice. Množinu L nazýváme *lineárním prostorem nad tělesem T*, pokud jsou definovány operace $+ : L \times L \to L$ a $\cdot : T \times L \to L$ tak, že L tvoří s operací $+$ komutativní grupu,

a dále $\forall \alpha, \beta \in T, \forall \boldsymbol{x}, \boldsymbol{y} \in L$:

$$
\begin{aligned}
&\text{(A)} \quad \alpha \cdot (\beta \cdot \boldsymbol{x}) = (\alpha \cdot \beta) \cdot \boldsymbol{x}, \\
&\text{(B)} \quad \alpha \cdot (\boldsymbol{x} + \boldsymbol{y}) = \alpha \cdot \boldsymbol{x} + \alpha \cdot \boldsymbol{y}, \\
&\text{(C)} \quad (\alpha + \beta) \cdot \boldsymbol{x} = \alpha \cdot \boldsymbol{x} + \beta \cdot \boldsymbol{x}, \\
&\text{(D)} \quad 1 \cdot \boldsymbol{x} = \boldsymbol{x}.
\end{aligned}
$$

15.40. Poznámka. Volíme-li za těleso T v této definici množinu reálných čísel $\mathbf{R}$, dostáváme vzhledem k poznámce ?? definici lineárního prostoru ??. Abych uklidnil čtenáře, tak konstatuji, že v dalších kapitolách tohoto textu nebudeme potřebovat lineární prostor v takové obecnosti (nad libovolným tělesem) a vystačíme si většinou s lineárním prostorem nad reálnými čísly. Pokud tedy nebude výslovně řečeno jinak (například lineární prostor nad $\mathbf{Z}_2$ studovaný v kapitole ??), pak pojmem *lineární prostor* myslíme lineární prostor nad $\mathbf{R}$ a stačí použít definici ??.

15.41. Příklad. Vrátíme se k příkladu lineárního prostoru reálných uspořádaných n-tic ?? a zobecníme ho na lineární prostor uspořádaných n-tic prvků libovolného tělesa.

Nechť T je těleso. Uvažujme množinu uspořádaných n-tic prvků z tělesa T (označme ji T^n) a definujme na ni operace $+ \colon T^n \times T^n \to T^n$, $\cdot \colon T \times T^n \to T^n$ takto: pro každé $(a_1, \ldots, a_n) \in T^n$, $(b_1, \ldots, b_n) \in T^n$, $\alpha \in T$ je

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) \stackrel{\text{df}}{=} (a_1 + b_1, \ldots, a_n + b_n),$$
$$\alpha \cdot (a_1, \ldots, a_n) \stackrel{\text{df}}{=} (\alpha \cdot a_1, \ldots, \alpha \cdot a_n).$$

Snadno se dá ověřit, že množina T^n s takto definovanými operacemi tvoří lineární prostor nad tělesem T.

15.42. Poznámka. Volíme-li za těleso $T = \mathbf{Z}_2$, je T^n podle předchozího příkladu diskrétní lineární prostor, který je používán v teorii kódování. Jednotlivé vektory (tzv. binární slova) jsou uspořádané n-tice jedniček a nul. Tento lineární prostor má celkem 2^n různých vektorů.

15.43. Poznámka. V případě lineárního prostoru nad konečným tělesem dostáváme konečný lineární prostor. V tomto případě tedy neplatí tvrzení poznámky ??. Můžete si všimnout, že toto tvrzení se opíralo o skutečnost, že „reálných čísel je nekonečně mnoho“. Poznámka ?? zůstává v platnosti pro lineární prostory nad nekonečnými tělesy.

16. Lineární algebra v teorii kódování

16.1. Poznámka. Teorie kódování řeší otázku, jak převést danou informaci do slov, která používají znaky nějaké abecedy (obvykle abecedy jedniček a nul) pokud možno efektivně, tj. bez zbytečného zatěžování přenosových linek a paměťových médií nadbytečnými informacemi. Typickým příkladem kódování je ASCII kód, který písmenům anglické abecedy a běžným znakům přiřazuje sedmibitová slova. Navíc se při kódování často řeší otázka, jakým způsobem efektivně přidat k zakódované informaci dodatečné bity tak, aby byla informace odolná vůči šumu na přenosové lince nebo menším chybám na paměťovém médiu. Dekodér, tj. zařízení, které má za úkol restaurovat původní informaci, může být postaven za nekvalitní linkou a může tedy dostat informaci zkreslenou. Z vhodně navržených dodatečných bitů může dekodér zjistit, zda informace při průchodu linkou byla poškozena a v lepším případě dokáže chybu také opravit.

Při návrhu vhodného kódování s možností detekce a opravy chyb se už od padesátých let minulého století používala lineární algebra. Tuto kapitolu završíme příkladem konstrukce tzv. lineárních Hammingových kódů. To samozřejmě zdaleka nepokrývá veškerou problematiku teorie kódování, zájemce o další studium této problematiky může použít třeba [1].

Někteří laici možná nerozlišují slovo kódování od slova šifrování. Šifrování je převod informace do takového stavu, aby ji bylo možné zpětně zrestaurovat jen pověřenými osobami. Tuto problematiku, ačkoli matematicky rovněž velmi zajímavou a ze strategického hlediska velmi důležitou, zde řešit nebudeme.

16.2. Poznámka. Definice lineárního prostoru ?? předpokládá, že skaláry (čísla, kterými násobíme vektory) jsou reálná čísla. V této kapitole budeme pracovat s modifikovanou definicí lineárního prostoru, kde reálná čísla nahradíme tělesem $\mathbf{Z}_2$.

Poznamenávám, že pojem tělesa jsem přesně zavedl v textu za poznámkou ??. Pokud čtenář tuto část textu přeskočil, může si pod pojmem těleso zhruba představit množinu s operacemi sčítání a násobení. Tyto operace mají podobné vlastnosti, jako sčítání a násobení reálných čísel (komutativita, asociativita, distributivita, atd.).

16.3. Definice. *Těleso* $\mathbf{Z}_2$ je dvoubodová množina $\{0,1\}$, na které je definováno sčítání $+\colon \mathbf{Z}_2 \times \mathbf{Z}_2 \to \mathbf{Z}_2$ a násobení $\cdot\colon \mathbf{Z}_2 \times \mathbf{Z}_2 \to \mathbf{Z}_2$ takto:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Tedy: $0+0=0$, $0+1=1+0=1$, $1+1=0$, $0\cdot 0=0\cdot 1=1\cdot 0=0$, $1\cdot 1=1$.

16.4. Poznámka. Sčítání na $\mathbf{Z}_2$ je shodné s logickou operací XOR (vylučovací nebo) a násobení na $\mathbf{Z}_2$ je shodné s operací AND (logická konjunkce).

Nebo jinak: Násobení na $\mathbf{Z}_2$ je stejné, jako jsme zvyklí násobit celá čísla, a sčítání skoro taky, až na jedinou výjimku: $1+1=0$.

Nebo ještě jinak: Prvek 0 v $\mathbf{Z}_2$ si můžeme představit jako jakékoli sudé číslo a prvek 1 jako jakékoli číslo liché. Sčítáme a násobíme pak sudá čísla se sudými, s lichými atd. Tyto operace pak dávají jako výsledek čísla sudá nebo lichá přesně podle pravidel počítání v $\mathbf{Z}_2$.

Nebo ještě jinak: provedeme operaci sčítání a násobení jako v případě celých čísel, ale pokud výsledek padne mimo množinu $\{0,1\}$, použijeme zbytek při dělení výsledku číslem 2.

16.5. Příklad. Na množině uspořádaných n-tic prvků ze $\mathbf{Z}_2$, tj. na množině $\mathbf{Z}_2^n$, zavedeme operaci sčítání $+\colon \mathbf{Z}_2^n \times \mathbf{Z}_2^n \to \mathbf{Z}_2^n$ analogicky, jako v případě sčítání uspořádaných n-tic reálných čísel, jen samozřejmě pracujeme se sčítáním podle definice ??. Pro $(a_1,\dots,a_n) \in \mathbf{Z}_2^n$ a $(b_1,\dots,b_n) \in \mathbf{Z}_2^n$ definujeme

$$(a_1,\dots,a_n) + (b_1,\dots,b_n) \stackrel{\text{df}}{=} (a_1+b_1,\dots,a_n+b_n).$$

Například $(1,0,0,1,1) + (1,1,0,0,1) = (0,1,0,1,0)$.

Dále definujeme násobení těchto uspořádaných n-tic jedničkou a nulou přirozeným způsobem:

$$1 \cdot (a_1,\dots,a_n) \stackrel{\text{df}}{=} (a_1,\dots,a_n), \qquad 0 \cdot (a_1,\dots,a_n) \stackrel{\text{df}}{=} (0,\dots,0).$$

Povšimněte si analogie s příklady ?? a ??.

Pokud nahradíme v definici lineárního prostoru ?? množinu reálných čísel $\mathbf{R}$ nějakým tělesem, pak takovému lineárnímu prostoru říkáme, že je definován „nad tělesem“ (podrobněji

viz definici ??). V tomto příkladě jsme zavedli na množině $\mathbf{Z}_2^n$ operace tak, že dostáváme *lineární prostor nad tělesem* $\mathbf{Z}_2$.

Nulový vektor tohoto lineárního prostoru je vektor $(0, \dots, 0)$. Tento lineární prostor má celkem 2^n vektorů, které mezi sebou umíme sčítat a samozřejmě tyto vektory umíme násobit jedničkou nebo nulou.

16.6. Poznámka. Na rozdíl od lineárních prostorů nad $\mathbf{R}$ náš nově zavedený lineární prostor nad $\mathbf{Z}_2$ má konečně mnoho prvků. To je jediný rozdíl vzhledem k lineárním prostorům, které jsme dosud studovali. Všechny ostatní vlastnosti zůstávají stejné.

16.7. Poznámka. Každý vektor z $\mathbf{Z}_2^n$ je sám sobě opačným vektorem, tj. $\forall \boldsymbol{x} \in \mathbf{Z}_2^n : \boldsymbol{x} = -\boldsymbol{x}$, neboli $\boldsymbol{x} + \boldsymbol{x} = \boldsymbol{o}$. Díky tomu v tělese $\mathbf{Z}_2$ a v lineárním prostoru nad tímto tělesem nemusíme rozlišovat mezi sčítáním a odčítáním.

16.8. Příklad. Najdeme dimenzi a bázi lineárního obalu čtyř vektorů v $\mathbf{Z}_2^5$:

$$M = \langle (1,0,1,0,1), (1,1,0,0,1), (1,0,0,1,1), (0,1,1,0,0) \rangle.$$

Řešení: Protože Gaussova eliminace nemění lineární obal, najdeme bázi eliminací:

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

Báze M je tedy například $(1,0,1,0,1), (0,1,1,0,0), (0,0,1,1,0)$. Dimenze M je tři.

16.9. Poznámka. Protože $\mathbf{Z}_2^n$ obsahuje konečný počet vektorů, můžeme (na rozdíl od lineárních prostorů nad $\mathbf{R}$) vypsat podprostor nebo lineární obal výčtem prvků. Pro podprostor M z předchozího příkladu platí:

$$M = \{(0,0,0,0,0), (1,0,1,0,1), (0,1,1,0,0), (0,0,1,1,0),\\ (1,1,0,0,1), (1,0,0,1,1), (0,1,0,1,0), (1,1,1,1,1)\}.$$

Jak se dá takový výčet prvků najít? Především pro $\boldsymbol{x} \neq \boldsymbol{o}$ je $\langle \boldsymbol{x} \rangle = \{\boldsymbol{o}, \boldsymbol{x}\}$. Skutečně, vektor $\boldsymbol{x}$ můžeme násobit jen jedničkou nebo nulou. To jsou všechny lineární kombinace, které můžeme s vektorem $\boldsymbol{x}$ vytvořit. Množina M má tříprvkovou bázi $\{\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}\}$. Takže pro sestavení lineárního obalu stačí najít všechny lineární kombinace těchto tří vektorů: $\boldsymbol{o},\ \boldsymbol{a},\ \boldsymbol{b},\ \boldsymbol{c},\ \boldsymbol{a}+\boldsymbol{b},\ \boldsymbol{a}+\boldsymbol{c},\ \boldsymbol{b}+\boldsymbol{c},\ \boldsymbol{a}+\boldsymbol{b}+\boldsymbol{c}$.

16.10. Příklad. Zjistěte počet prvků lineárního (pod)prostoru nad $\mathbf{Z}_2$, který má dimenzi n.

Řešení: Má-li (pod)prostor dimenzi n, pak má n prvkovou bázi $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n$. Abychom získali všechny lineární kombinace těchto vektorů, musíme každý vektor násobit jedničkou nebo nulou. Máme tedy 2^n lineárních kombinací. Tyto kombinace vyplňují celý lineární (pod)prostor a jsou navzájem různé. Kdyby se totiž dvě lineární kombinace s různými koeficienty rovnaly, pak jejich odečtením dostáváme netriviální lineární kombinaci rovnu nulovému vektoru. To je spor se skutečností, že $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n$ je báze.

Závěr: počet prvků lineárního (pod)prostoru nad $\mathbf{Z}_2$ dimenze n je 2^n. Například podprostor M z příkladu ?? má dimenzi 3 a má tedy $2^3 = 8$ prvků.

16.11. Příklad. Najděte všechna řešení $\boldsymbol{x} \in \mathbf{Z}_2^6$ homogenní soustavy rovnic $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$, je-li

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

Řešení: Najdeme matici ekvivalentní soustavy s lineárně nezávislými řádky:

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

Hodnost matice soustavy je 4, dimenze prostoru je 6, takže dimenze množiny řešení je 2. Hledáme tedy dvě lineárně nezávislá řešení: $(?,?,?,?,1,0)$ a $(?,?,?,?,0,1)$. Dosazením „zespoda nahoru“ dostáváme následující řešení: $(0,1,1,1,1,0)$, $(0,1,0,0,0,1)$.

Množina všech řešení je lineárním obalem těchto dvou řešení a obsahuje $2^2 = 4$ vektory:

$$\langle (0,1,1,1,1,0), (0,1,0,0,0,1) \rangle = \{(0,0,0,0,0,0), (0,1,1,1,1,0), (0,1,0,0,0,1), (0,0,1,1,1,1)\}.$$

16.12. Poznámka. Při hledání báze prostoru řešení můžeme také využít větu ??. V předchozím příkladě bychom pak pokračovali v eliminaci zpětným chodem:

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

Tvar matice $(\mathbf{E}|\mathbf{C})$ odpovídá předpokladu věty ??, takže řádky báze řešení tvoří matici:

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

Poznamenejme, že nemusíme přecházet od matice $\mathbf{C}$ k matici $-\mathbf{C}$, protože v aritmetice $\mathbf{Z}_2$ jsou obě matice stejné.

16.13. Definice. Nechť A je konečná množina (tzv. *abeceda*). Pak *slovo* je libovolná konečná posloupnost prvků z A.

Kódování v obecném smyslu zahrnuje (1) algoritmus, kterým informace převádíme do posloupnosti slov (tzv. *kodér*) a (2) algoritmus, kterým zpětně z těchto slov získáváme původní informaci (*dekodér*).

Slova, která vytváří kodér, se nazývají *kódová slova*. Množina všech kódových slov se nazývá *kód*.

Je-li kód množinou slov stejné délky (každé kódové slovo má stejný počet znaků abecedy), mluvíme o tzv. *blokovém kódu*. Blokový kód *délky n* značí, že všechna kódová slova mají n znaků abecedy.

16.14. Poznámka. Typicky $A = \{0, 1\}$, tj. abeceda se skládá jen ze dvou znaků (tzv. bitů, anglicky bits, což je původně zkratka z BInary digiTS) a slova jsou posloupnosti těchto bitů.

16.15. Příklad. ASCII kód je množina 7bitových slov, která reprezentují jednotlivá písmena anglické abecedy a další běžné znaky (číslice, tečku, vykřičník, otazník, mezeru, `#` neboli vězení atd.). Tato množina obsahuje 91 slov, protože v době vzniku tohoto kódu byl požadavek na kódování 91 znaků. Kodér i dekodér pak pracují s tabulkou těchto znaků, u kterých jsou uvedena odpovídající kódová slova. Tato tabulka může být na straně kodéru technicky realizována třeba ovladačem klávesnice a na straně dekodéru fontem.

Jedná se o blokový kód. Od počátku existence počítačů byl tento blokový kód rozšířen o redundantní nulový bit na začátku, takže často je ASCII kód prezentován jako množina 8bitových slov. Později začal být tento bit využíván pro různá rozšíření ASCII kódu, která zahrnují i reprezentaci některých písmen s diakritickými znaménky.

16.16. Poznámka. Je potřeba si uvědomit, že slova jsou do paměťového média nebo do přenosové linky vkládána za sebou bez oddělovačů. Blokový kód má tu výhodu, že dekodér dokáže snadno rozdělit tento „tok znaků abecedy“ na slova a těm pak přidělit význam například pomocí nějaké tabulky. Nevýhoda blokového kódu spočívá v tom, že plýtvá místem, neboť tušíme, že pokud navrhneme pro častěji se vyskytující slova kratší posloupnosti znaků, celkový počet znaků abecedy pro přenášené/ukládané informace může být menší. To ostatně je (alespoň zhruba) i vlastnost přirozeného jazyka. Tam máme ovšem abecedu rozsáhlejší (nebinární) a za prvek abecedy můžeme považovat i mezeru: oddělovač mezi slovy, který dekodéru pomůže. Nebo v Morseově abecedě máme také tři znaky: tečka, čárka a mezera. Bez mezery by bylo dekódování morseovky nemožné. Máme-li k dispozici jen binární abecedu $A = \{0, 1\}$, pak je potřeba při návrhu kódu se slovy nestejné délky myslet na možnosti dekodéru. Je to technicky možné, ale není to obsahem tohoto textu. Příkladem neblokového kódu je UTF8, který kóduje znaky abeced všech jazyků světa. Písmena anglické abecedy a běžné znaky jsou reprezentovány 8bitovým slovem, ale písmena dalších jazyků jsou kódována 16bitovým slovem nebo i delším (24 bitů a 32 bitů).

Nadále budeme pracovat jen s blokovými kódy nad binární abecedou.

16.17. Poznámka. Nechť K je blokový kód délky n nad binární abecedou A. Pak platí $K \subseteq A^n$.

Pokud $K \neq A^n$, pak mezi uspořádanými n-ticemi z A existují nekódová slova, tj. taková, která kodér nikdy nevytvoří a která nemají přidělen význam. Přijme-li dekodér (např. za

nekvalitní linkou) nekódové slovo, je si jist, že při přenosu linkou došlo k chybě. Může například v takovém případě požádat pomocí jiných technických prostředků kodér, aby vyslal slovo znovu. Nebo se může pokusit chybu opravit.

Tušíme jisté problémy: šum na lince může způsobit tak nešťasnou chybu, že se z jednoho kódového slova stane jiné kódové slovo a dekodér nic nepozná. Je tedy rozumné kódování navrhnout tak, aby například omezený počet chyb v jednom slově (tj. záměn nuly za jedničku a naopak) zaručil, že se z kódového slova stane slovo nekódové.

Znovu můžeme hledat analogii v přirozeném jazyce. Překlep ve slově jsme velmi často schopni detekovat i opravit. Někdy ale překlep může způsobit, že vzniká jiné běžné slovo jazyka. Člověk jako dekodér ani s tímto druhem chyby nemá většinou problém, protože pracuje s kontextem celé věty (větší skupiny slov). Takto inteligentní dekodér ale nebude naším cílem. Vystačíme si s detekováním a opravováním chyb jen na úrovni jednotlivých slov.

16.18. Definice. Nechť $A = \{0, 1\}$. *Hammingova velikost slova* $\boldsymbol{u} \in A^n$ je počet jedniček v tomto slově a značíme ji $\|\boldsymbol{u}\|$. *Hammingova vzdálenost slov* $\boldsymbol{v} \in A^n$ *a* $\boldsymbol{w} \in A^n$ je počet bitů, ve kterých se tato dvě slova liší. Značíme ji $\mathrm{d}(\boldsymbol{v}, \boldsymbol{w})$.

16.19. Poznámka. Nechť $A = \{0, 1\}$ a $\boldsymbol{v}, \boldsymbol{w} \in A^n$. Pak $\boldsymbol{v} + \boldsymbol{w}$ (v aritmetice $\mathbf{Z}_2$) je slovo, které má jedničky právě v místech, kde se $\boldsymbol{v}$ a $\boldsymbol{w}$ liší. Takže platí: $\mathrm{d}(\boldsymbol{v}, \boldsymbol{w}) = \|\boldsymbol{v} + \boldsymbol{w}\|$.

16.20. Poznámka. Předpokládejme, že $\boldsymbol{v}$ je slovo vyslané kodérem a $\boldsymbol{w}$ slovo přijaté dekodérem. Pak $\mathrm{d}(\boldsymbol{v}, \boldsymbol{w})$ udává počet chyb ve slově, které vznikly během přenosu.

Poznámka v poznámce: předpokládáme, že díky technickým parametrům zařízení nikdy nedojde k chybě, kdy se jednička nebo nula ze slova zcela vytratí nebo vznikne nová, tj. nikdy nehrozí riziko, že by na straně dekodéru byl přečten jiný počet jedniček a nul než byl vyslán kodérem.

16.21. Příklad. Je dán tento kód: $K = \{0000, 0011, 0101, 1001, 0110, 1010, 1100, 1111\}$. Jedná se o blokový binární kód délky 4. Pro potřeby tohoto příkladu nebudeme specifikovat druh informace, kterou potřebujeme přenášet. Protože kód obsahuje jen 8 slov, může být původní informace zapsána pomocí nějaké 8 znakové abecedy.

Zajímavé na tomto kódu je, že každé kódové slovo obsahuje sudý počet jedniček. Pokud dojde k jediné chybě ve slovu, máme jistotu, že dekodér přijme nekódové slovo (s lichým počtem jedniček) a ohlásí chybu. Je-li pravděpodobnost výskytu dvou nebo více chyb v jednom slově zanedbatelná a nám postačuje jen detekovat chyby (neopravovat je), je toto rozumný návrh kódu.

Povšimneme si, že minimální Hammingova vzdálenost mezi dvěma různými kódovými slovy tohoto kódu je 2, takže jedna chyba způsobí vytvoření nekódového slova.

16.22. Příklad. Je dán blokový kód délky 8 bitů: $K = \{00000000, 00001111, 11110000, 1111111$
Minimální Hammingova vzdálenost mezi kódovými slovy je 4, takže ani tři chyby ve slově

nezpůsobí přechod na jiné kódové slovo a dekodér správně detekuje chybu přenosu. Dekodér dokonce dokáže v tomto kódu opravit jednu chybu a detekovat výskyt dvou chyb ve slově. Chybu opraví tak, že se od přijatého slova $\boldsymbol{w}$ vrátí ke kódovému slovu $\boldsymbol{v}$ takovému, že Hammingova vzdálenost $\mathrm{d}(\boldsymbol{v},\boldsymbol{w}) = 1$. Samozřejmě, naučíme-li dekodér opravovat jednu chybu ve slově, pak už nemusí být schopen vždy správně detekovat tři chyby. Může se totiž stát, že místo toho opraví jeden bit a dostane jiné kódové slovo.

16.23. Příklad. Nechť minimální Hammingova vzdálenost mezi kódovými slovy je $d > 2$. Rozhodněte (A) kolik chyb ve slově může dekodér detekovat, pokud po něm nechceme, aby chyby opravoval, a (B) kolik chyb ve slově může opravit a kolik jich může aspoň detekovat bez opravy.

Odpověď: (A) Dekodér může spolehlivě detekovat nejvýše $d-1$ chyb. (B) Je-li d sudé, může dekodér opravit jednu až $d/2-1$ chyb a detekovat $d/2$ chyb bez opravy. Je-li d liché, může opravit jednu až $(d-1)/2$ chyb a žádné množství chyb nedetekuje bez opravy. Je samozřejmě možné i jiné rozvržení. Např. pro d liché necháme dekodér opravit nejvýše $(d-3)/2$ chyb a při výskytu $(d-1)/2$ nebo $(d+1)/2$ chyb ve slově jen chyby detekujeme bez opravy.

16.24. Poznámka. Při návrhu dekodéru s detekcí nebo opravou chyb se s výhodou využijí nástroje lineární algebry, jako je násobení matic, vymezení podprostorů a bází, řešení homogenních soustav atd. Binární slova délky n budeme v tomto případě považovat za vektory z lineárního prostoru $\mathbf{Z}_2^n$, takže je můžeme sčítat. Ostatně, už v poznámce ?? jsem zmínil

sčítání slov $\boldsymbol{v}$ a $\boldsymbol{w}$. V teorii kódování se binární slova zapisují jedničkami a nulami bez mezer (viz příklady ?? a ??), zatímco v lineární algebře jsme dosud zapisovali vektory do závorek a jejich složky oddělovali čárkami. Věřím, že nedojde k nedorozumění, pokud dále v textu o kódování budu zapisovat vektory způsobem, jako v příkladu ??.

16.25. Definice. Binární blokový kód K délky n je *lineární*, pokud K tvoří lineární podprostor lineárního prostoru $\mathbf{Z}_2^n$. Jestliže dimenzi tohoto podprostoru označíme k, pak mluvíme o *lineárním* (n, k) *kódu*.

16.26. Věta. Nejmenší Hammingova vzdálenost mezi slovy lineárního kódu K je rovna nejmenší Hammingově velikosti nenulového kódového slova.

Důkaz. Stačí si uvědomit, že pro $\boldsymbol{v}_1, \boldsymbol{v}_2 \in K$ je $\|\boldsymbol{v}_1 + \boldsymbol{v}_2\| = \mathrm{d}(\boldsymbol{v}_1, \boldsymbol{v}_2)$, a přitom $\boldsymbol{v}_1 + \boldsymbol{v}_2 \in K$, protože K je lineární kód. Navíc $\|\boldsymbol{v}\| = \mathrm{d}(\boldsymbol{v}, \boldsymbol{o})$.

16.27. Příklad. Kód z příkladu ?? je lineární, protože K tvoří podprostor lineárního prostoru $\mathbf{Z}_2^4$. Skutečně, sečteme-li dva vektory se sudým počtem jedniček, dostaneme vektor se sudým počtem jedniček. Výsledek násobení vektoru z K konstantou α zůstane v K, protože v $\mathbf{Z}_2$ číslo α může být jen 0 nebo 1.

Báze kódu z příkladu ?? je například $\{0011, 0101, 1100\}$, takže dimenze kódu je 3 a jedná se tedy o *lineární* $(4, 3)$ *kód*.

16.28. Poznámka. Příklad ?? ilustruje tzv. kódování s kontrolním bitem parity. Původní informaci s osmi znaky je možné kódovat blokovým binárním kódem $\{000, 001, 010, 011, 100, 101, 1$ tedy stačí nám tři bity. Pokud chceme detekovat jednu chybu ve slově, přidáme čtvrtý tzv. *kontrolní bit*, který nastavíme na 0, pokud je v původním tříbitovém slově sudý počet jedniček a nastavíme ho na 1, pokud je v původním slově lichý počet jedniček. Dostáváme tak kód z příkladu ??.

Tento postup můžeme použít na jakýkoli „výchozí“ binární blokový kód délky k se všemi 2^k kódovými slovy. Přidáním kontrolního bitu parity dostáváme lineární $(k+1, k)$ kód, kterým jsme schopni detekovat jednu chybu ve slově. Dekodér pak odstraní kontrolní bit z každého přijatého slova a získá tím původní kódovanou informaci.

16.29. Poznámka. Vstupní informace je často připravena už jako posloupnost slov binárního blokového kódu délky k, ve kterém všechna slova jsou kódová. Naším úkolem je pak rozšířit tento kód o dalších $n-k$ tzv. *kontrolních bitů*, abychom dostali lineární (n, k) kód. Kodér tedy očekává na vstupu libovolné slovo délky k a jeho úkolem je zkopírovat bity vstupu do výstupu (tzv. *informační bity*) a přidat $n - k$ kontrolních bitů. Dekodér pak použije tyto kontrolní bity pro detekci a případnou opravu chyb a poté je odstraní a ponechá jen informační bity. Cílem je navrhnout kódování, které má co nejmenší *redundanci* (tj. poměr počtu kontrolních bitů ku počtu všech přenášených bitů ve slově), protože ta zatěžuje linku nebo paměťové médium režijními informacemi, které uživatel ze svého pohledu nevyužije. Přitom ale chceme

co nejschopnější dekodér, který by detekoval a opravoval chyby a navíc by měl pracovat efektivně.

Z pohledu lineární algebry je výše popsaný přechod od kódu délky k na lineární kód délky $n > k$ lineární zobrazení $\mathcal{A}\colon \mathbf{Z}_2^k \to \mathbf{Z}_2^n$, které je prosté (jinak by docházelo ke ztrátě informace). Podle poznámky ?? množina obrazů tohoto zobrazení (neboli kód) tvoří lineární podporostor v $\mathbf{Z}_2^n$. Bázi tohoto podprostoru můžeme hledat tak, že sepíšeme bázi ve výchozím prostoru $\mathbf{Z}_2^k$ a najdeme její obraz za použití zobrazení $\mathcal{A}$. Tento obraz podle věty ?? jednoznačně určuje zobrazení $\mathcal{A}$ na celém $\mathbf{Z}_2^k$.

Kodérem je přímo zobrazení $\mathcal{A}$ a možným dekodérem je zobrazení inverzní k $\mathcal{A}$ definované na $\mathcal{A}(Z_2^k)$. Ovšem dekodér se musí umět vyrovnat i se slovy, která jsou nekódová, tj. neleží v množině $\mathcal{A}(Z_2^k)$. To inverzní zobrazení k $\mathcal{A}$ neumí.

16.30. Příklad. Nechť je vstupní informace kódována binárním blokovým kódem délky k se všemi 2^k slovy. Kodér této informace navrhneme tak, že každé vstupní slovo zopakuje a vytvoří výstupní slovo délky $2k$. Tím vzniká lineární $(2k, k)$ kód. Minimální Hammingova vzdálenost mezi dvěma kódovými slovy je 2, takže dekodér spolehlivě detekuje jednu chybu ve slově. Za jistých okolností může detekovat i více chyb ve slově, pokud chyba v první polovině slova se nezopakuje na stejném bitu druhé poloviny slova. V žádném případě ale dekodér nemůže odhalenou chybu spolehlivě opravit. Redundance je příliš vysoká, a přitom neumíme ani opravit chyby. Asi to nebude nejlepší možný návrh kódování.

16.31. Příklad. Kód z příkladu ?? je lineární. Nevýhoda tohoto kódu ale spočívá v tom, že kódová slova mohou reprezentovat jen čtyři rozdílné stavy původní informace, ale mají příliš mnoho bitů, které zbytečně zatěžují paměťové médium nebo přenosové linky. Proto se Hamming zaměřil na hledání jiných vhodnějších lineárních kódů.

16.32. Definice. *Generující matice lineárního kódu K* je po řádcích zapsaná báze tohoto kódu.

Kontrolní matice lineárního kódu K je taková matice $\mathbf{H}$ s lineárně nezávislými řádky, pro kterou platí: množina řešení homogenní soustavy $\mathbf{H}\,\boldsymbol{x} = \boldsymbol{o}$ je rovna kódu K.

16.33. Věta. Nechť $\mathbf{G}$ je generující matice a $\mathbf{H}$ kontrolní matice lineárního (n, k) kódu. Pak $\mathbf{G}$ má k řádků a $\mathbf{H}$ má $n - k$ řádků. Obě matice mají n sloupců. Jinými slovy, generující matice má tolik řádků, kolik je v kódu informačních bitů, kontrolní matice má tolik řádků, kolik má kód kontrolních bitů a počet sloupců obou matic je roven počtu přenášených bitů v jednom slově.

Důkaz. Matice $\mathbf{G}$ má k řádků, protože báze prostoru dimenze k obsahuje k vektorů. Počet řádků matice H plyne z věty ??. Konečně n sloupců obou matic plyne přímo z definice těchto matic.

16.34. Příklad. Kód z příkladu ?? může mít následující generující matici:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

protože $\{1001, 0101, 0011\}$ je báze kódu K. Popíšu, jak se obvykle tato báze sestavuje. Vyjde se ze standardní báze vstupního kódu: $\{100, 010, 001\}$ a aplikuje se na ní zobrazení kodéru. Všechny tři prvky této báze mají lichý počet jedniček, takže poslední kontrolní bit kodér nastaví na jedničku.

Kontrolní matice našeho kódu je

$$\mathbf{H} = (\,1 \quad 1 \quad 1 \quad 1\,),$$

protože množina řešení rovnice $x_1 + x_2 + x_3 + x_4 = 0$ je shodná s množinou slov, které mají sudý počet jedniček (sčítáme jedničky modulo 2), a to jsou právě všechna kódová slova.

16.35. Příklad. Kódujme vstupní informaci v blokovém kódu délky 4 podle příkladu ?? (zdvojení slova). Dostáváme lineární (8,4) kód. Jeho generující matice je

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

K vytvoření této báze jsem použil stejný postup, jako v předchozím příkladě. Na standardní bázi prostoru $\mathbf{Z}_2^4$ jsem aplikoval zobrazení kodéru. Kontrolní matice je výjimečně v tomto příkladě $\mathbf{H} = \mathbf{G}$, protože soustava rovnic

$$\begin{aligned} x_1 + x_5 &= 0 \\ x_2 + x_6 &= 0 \\ x_3 + x_7 &= 0 \\ x_4 + x_8 &= 0 \end{aligned}$$

má za řešení právě taková slova, pro která první bit je roven pátému, druhý šestému, třetí sedmému a čtvrtý osmému, tj. obě části slova se rovnají a jedná se o kódové slovo.

16.36. Poznámka. Generující matice sama o sobě jednoznačně určuje lineární kód. Kontrolní matice sama o sobě také jednoznačně určuje lineární kód. Tyto dvě matice jsou v následujícím „duálním“ vztahu:

16.37. Věta. Nechť $\mathbf{G}$ je generující a $\mathbf{H}$ je kontrolní matice lineárního (n, k) kódu. Pak $\mathbf{H} \cdot \mathbf{G}^T = \mathbf{O}_1$ a také $\mathbf{G} \cdot \mathbf{H}^T = \mathbf{O}_2$, kde $\mathbf{O}_1$ je nulová matice s $n - k$ řádky a k sloupci a $\mathbf{O}_2 = \mathbf{O}_1^T$.

Důkaz. Kód s uvedenými maticemi označíme písmenem K. Řádky matice $\mathbf{G}$ alias sloupce matice $\mathbf{G}^T$ jsou podle definice generující matice prvky kódu K. Podle definice kontrolní matice

musí tyto sloupce matice $\mathbf{G}^T$ alias prvky kódu K být řešením soustavy $\mathbf{H}\,\boldsymbol{x} = \boldsymbol{o}$. Přesně to říká vztah $\mathbf{H} \cdot \mathbf{G}^T = \mathbf{O}_1$, pokud jej rozepíšeme po jednotlivých sloupcích matice $\mathbf{G}^T$.

Vztah $\mathbf{G} \cdot \mathbf{H}^T = \mathbf{O}_2$ vzniká transponováním matic na levé i pravé straně vztahu $\mathbf{H} \cdot \mathbf{G}^T = \mathbf{O}_1$.

16.38. Poznámka. Předchozí věta ukazuje, že nejen řádky matice $\mathbf{G}$ řeší soustavu $\mathbf{H}\boldsymbol{x} = \boldsymbol{o}$, ale také řádky matice $\mathbf{H}$ řeší soustavu $\mathbf{G}\boldsymbol{x} = \boldsymbol{o}$. Známe-li jen jednu z těchto matic, pak druhou lze najít tak, že najdeme bázi množiny řešení odpovídající homogenní soustavy rovnic a zapíšeme ji do řádků.

Protože velmi často je generující matice vytvořena za použití standardní báze vstupního prostoru $\mathbf{Z}_2^k$ a aplikací algoritmu kodéru na tuto bázi, který kopíruje informační bity a přidává kontrolní bity na konec slova, je matice $\mathbf{G}$ často ve tvaru $\mathbf{G} = (\mathbf{E}|\mathbf{C})$, kde $\mathbf{E}$ je jednotková matice typu (k, k). Matici $\mathbf{H}$ pak můžeme snadno najít podle věty ??, přitom místo matice $-\mathbf{C}^T$ stačí použít matici $\mathbf{C}^T$, protože v aritmetice $\mathbf{Z}_2$ je $\mathbf{C} = -\mathbf{C}$. Dostáváme $\mathbf{H} = (\mathbf{C}^T|\mathbf{E}')$, kde $\mathbf{E}'$ je jednotková matice typu $(n-k, n-k)$.

16.39. Příklad. S využitím věty ?? zkusíme sestavit kontrolní matice z příkladů ?? a ??, pokud je dána jen generující matice.

Příklad ??. Matice $\mathbf{C}$ z rovnosti $\mathbf{G} = (\mathbf{E}|\mathbf{C})$ obsahuje sloupec jedniček. $\mathbf{C}^T$ je tedy řádek jedniček, ke kterému podle věty ?? vpravo připíšeme jednotkovou matici typu $(1, 1)$. Dostáváme matici $\mathbf{H}$.

Příklad ??. Matice $\mathbf{C}$ z rovnosti $\mathbf{G} = (\mathbf{E}|\mathbf{C})$ je jednotková matice, takže $\mathbf{C}^T = \mathbf{C}$. K této jednotkové matici podle věty ?? připíšeme jednotkovou matici typu $(4, 4)$. Dostáváme tím matici $\mathbf{H}$, která je výjimečně rovna matici $\mathbf{G}$.

16.40. Definice. Pokud existuje generující matice lineárního kódu ve tvaru $\mathbf{G} = (\mathbf{E}|\mathbf{C})$, kde $\mathbf{E}$ je jednotková matice, nazýváme takový kód *systematický*.

16.41. Poznámka. Předchozí poznámka ?? ukazuje, že pro systematické kódy můžeme z generující matice snadno sestavit matici kontrolní ve tvaru $\mathbf{H} = (\mathbf{C}^T|\mathbf{E}')$. Také obráceně, pokud je dána kontrolní matice ve tvaru $\mathbf{H} = (\mathbf{C}^T|\mathbf{E}')$, je možné snadno přejít k matici generující tvaru $\mathbf{G} = (\mathbf{E}|\mathbf{C})$.

16.42. Poznámka. Nechť je dána generující matice, která není tvaru $(\mathbf{E}|\mathbf{C})$. Protože generující matice obsahuje v řádcích bázi kódu, je možné eliminací této matice přejít k jiné generující matici téhož kódu. Stačí si uvědomit, že Gaussova eliminace nemění lineární obal řádků. Může se tedy stát, že po eliminaci dostaneme novou generující matici ve tvaru $\mathbf{G} = (\mathbf{E}|\mathbf{C})$ a shledáme, že kód je systematický.

Pokud ani po eliminaci generující matice nelze dosáhnout tvaru $(\mathbf{E}|\mathbf{C})$, jedná se o nesystematický kód. I v tomto případě je ovšem eliminací možné dospět k matici, která se od matice $(\mathbf{E}|\mathbf{C})$ liší jen prohozením některých sloupců. Nesystematický kód se tedy od systematického liší jen pořadím bitů v jednotlivých kódových slovech. Přechod od generující matice ke

kontrolní (nebo obráceně) je u nesystematického kódu obtížnější, protože nelze přímo použít větu ??, ale před jejím použitím musíme prohodit sloupce generující matice, pak přejít ke kontrolní matici a u ní prohodit sloupce zpět. Podobně bychom postupovali, pokud přecházíme od kontrolní matice nesystematického kódu k matici generující.

Systematický kód získáme zaručeně v případě, kdy necháme kodér kopírovat informační bity vstupního slova do výstupu a pak přidat bity kontrolní. Pokud ale kodér informační bity „promíchá“ s bity kontrolními, pak kód nemusí být systematický.

16.43. Věta. Kód je systematický právě tehdy, když existuje kontrolní matice tohoto kódu tvaru $(\mathbf{C}^T|\mathbf{E}')$, kde $\mathbf{E}'$ je jednotková matice.

Důkaz. Tvrzení věty je důsledkem skutečnosti, že kód má generující matici tvaru $\mathbf{G} = (\mathbf{E}|\mathbf{C})$ právě tehdy, když má kontrolní matici tvaru $\mathbf{H} = (\mathbf{C}^T|\mathbf{E}')$.

16.44. Poznámka. Je-li dána kontrolní matice v jiném tvaru než $(\mathbf{C}^T|\mathbf{E}')$, pak z toho ještě neplyne, že kód není systematický. Eliminací kontrolní matice můžeme získat jinou kontrolní matici, která ovšem přísluší stejnému kódu. Stačí si uvědomit, že eliminací matice soustavy dostáváme případně matici jiné soustavy, ale se stejnou množinou řešení. Pokud tedy po eliminaci kontrolní matice získáme matici tvaru $(\mathbf{C}^T|\mathbf{E}')$, pak je kód systematický.

16.45. Věta. Nechť $\mathbf{G}$ je generující matice lineárního (n, k) kódu. Nechť dále $\mathcal{A}\colon \mathbf{Z}_2^k \to \mathbf{Z}_2^n$ je lineární zobrazení, které zobrazuje standardní bázi prostoru $\mathbf{Z}_2^k$ na řádky matice $\mathbf{G}$. Pak matice $\mathbf{G}^T$ je maticí lineárního zobrazení $\mathcal{A}$ vzhledem ke standardním bázím.

Důkaz. Matice lineárního zobrazení obsahuje podle definice ?? ve sloupcích souřadnice obrazů báze vstupního prostoru vzhledem k bázi výstupního prostoru. V našem případě generující matice $\mathbf{G}$ obsahuje v řádcích souřadnice obrazů (při zobrazení $\mathcal{A}$) standardní báze $\mathbf{Z}_2^k$ vzhledem ke standardní bázi v $\mathbf{Z}_2^n$. Abychom z řádků matice dostali sloupce podle definice matice lineárního zobrazení, stačí matici $\mathbf{G}$ transponovat.

16.46. Poznámka. Zobrazení $\mathcal{A}$ z předchozí věty matematicky popisuje kodér lineárního kódu. Jeho generující matice je $\mathbf{G}$. Věta říká, že $\mathbf{G}^T$ je matice zobrazení tohoto kodéru vzhledem ke standardním bázím. Vstupuje-li vektor $\boldsymbol{u} \in \mathbf{Z}_2^k$ do kodéru, pak jeho výstupem je vektor $\boldsymbol{v} \in \mathbf{Z}_2^n$, který spočítáme podle věty ?? jako součin matice zobrazení a vstupního vektoru:

$$\boldsymbol{v}^T = \mathbf{G}^T \cdot \boldsymbol{u}^T, \qquad \text{neboli:} \quad \boldsymbol{v} = \boldsymbol{u} \cdot \mathbf{G}.$$

16.47. Poznámka. Pokud kodér kopíruje k vstupních bitů do výstupu a pak přidá kontrolní bity, nemusíme prvních k bitů výstupu počítat maticovým násobením. Stačí tímto násobením počítat kontrolní bity. Generující matice má v tomto případě tvar $\mathbf{G} = (\mathbf{E}|\mathbf{C})$. Označíme-li

$\boldsymbol{u}$ slovo, které vstupuje do kodéru a $\boldsymbol{v}'$ vektor, který obsahuje jen kontrolní bity výstupního slova, pak platí:

$$\boldsymbol{v}' = \boldsymbol{u} \cdot \mathbf{C}.$$

16.48. Poznámka. Dekodér při kontrole, zda se jedná o kódové slovo, použije kontrolní matici. Nechť dekodér přijme slovo $\boldsymbol{w}$. Pak $\mathbf{H} \cdot \boldsymbol{w}^T$ je nulový vektor právě tehdy, když je slovo $\boldsymbol{w}$ kódové. V takovém případě dekodér předpokládá, že nedošlo při přenosu slova k chybě, odstraní kontrolní bity a tím získá původní informaci.

Pokud $\mathbf{H} \cdot \boldsymbol{w}^T$ není nulový vektor, dekodér má jistotu, že došlo k chybě a že $\boldsymbol{w}$ není kódové slovo. Má-li chybu opravit, pak údaj $\mathbf{H} \cdot \boldsymbol{w}^T$ bude při opravě potřebovat. Napíšeme-li výsledek násobení $\mathbf{H} \cdot \boldsymbol{w}^T$ do řádku, dostáváme tzv. *syndrom* vektoru $\boldsymbol{w}$.

16.49. Definice. Nechť $\mathbf{H}$ je kontrolní matice lineárního kódu. *Syndrom* slova $\boldsymbol{w}$ je vektor $\boldsymbol{s}$, pro který platí $\boldsymbol{s}^T = \mathbf{H} \cdot \boldsymbol{w}^T$.

Nechť $\boldsymbol{v}$ je slovo vyslané kodérem a $\boldsymbol{w}$ je slovo přijaté dekodérem. Pak $\boldsymbol{e} = \boldsymbol{w} - \boldsymbol{v}$ je *chybové slovo*. Protože v $\mathbf{Z}_2^n$ je $-\boldsymbol{v} = \boldsymbol{v}$, chybové slovo lze počítat jako $\boldsymbol{w} + \boldsymbol{v}$.

16.50. Poznámka. Jedničkové bity chybového slova označují místa, kde došlo k poškození slova $\boldsymbol{v}$. Úkolem dekodéru je na základě znalosti $\boldsymbol{w}$ zjistit chybové slovo $\boldsymbol{e}$. Pokud se mu to podaří, pak vypočte původní informaci jako $\boldsymbol{v} = \boldsymbol{w} - \boldsymbol{e}$.

Než se pustíme do sestavování tabulky, podle které bude dekodér opravovat chyby, je potřeba si uvědomit platnost dvou tvrzení. První z nich platí dokonce obecně na libovolném lineárním prostoru.

16.51. Věta. Nechť K je lineární podprostor lineárního prostoru L a nechť $\boldsymbol{e}_1 \in L$, $\boldsymbol{e}_2 \in L$. Pak množiny $M_1 = \{\boldsymbol{e}_1 + \boldsymbol{v};\ \boldsymbol{v} \in K\}$, $M_2 = \{\boldsymbol{e}_2 + \boldsymbol{v};\ \boldsymbol{v} \in K\}$ jsou buď disjunktní nebo totožné.

Důkaz. Sporem. Předpokládáme, že množiny M_1 a M_2 mají společný bod $\boldsymbol{a}$ a přitom nejsou totožné, tj. existuje vektor $\boldsymbol{b} \in M_1$, který neleží v M_2. Protože $\boldsymbol{a}$ i $\boldsymbol{b}$ leží v množině M_1, je $\boldsymbol{a} = \boldsymbol{e}_1 + \boldsymbol{u}$, $\boldsymbol{b} = \boldsymbol{e}_1 + \boldsymbol{v}$, kde $\boldsymbol{u}$ i $\boldsymbol{v}$ leží v K. Pak $\boldsymbol{w} = \boldsymbol{b} - \boldsymbol{a} = \boldsymbol{v} - \boldsymbol{u}$ leží v K, protože K je podprostor. Je tedy $\boldsymbol{b} = \boldsymbol{a} + \boldsymbol{w}$. Protože $\boldsymbol{a}$ leží i v množině M_2, je $\boldsymbol{a} = \boldsymbol{e}_2 + \boldsymbol{x}$, kde $\boldsymbol{x} \in K$. Dosadíme-li tento poznatek do vztahu pro $\boldsymbol{b}$, dostaneme $\boldsymbol{b} = \boldsymbol{e}_2 + \boldsymbol{x} + \boldsymbol{w}$. Protože K je podprostor, $\boldsymbol{x} + \boldsymbol{w}$ leží v K. Je tedy $\boldsymbol{b} = \boldsymbol{e}_2 + \boldsymbol{z}$, kde $\boldsymbol{z} \in K$. To ale znamená, že $\boldsymbol{b} \in M_2$, což je sporu s předpokladem.

16.52. Věta. Nechť $\boldsymbol{v}$ je kódové slovo a $\boldsymbol{e}$ je libovolné slovo. Pak slova $\boldsymbol{e}$ i $\boldsymbol{e} + \boldsymbol{v}$ mají stejný syndrom. Jinými slovy kódová slova modifikovaná stejnou chybou vytvářejí skupinu slov se společným syndromem.

Důkaz. $\mathbf{H} \cdot (\boldsymbol{e} + \boldsymbol{v})^T = \mathbf{H} \cdot \boldsymbol{e}^T + \mathbf{H} \cdot \boldsymbol{v}^T = \mathbf{H} \cdot \boldsymbol{e}^T + \boldsymbol{o}^T = \mathbf{H} \cdot \boldsymbol{e}^T$.

16.53. Poznámka. Pokud požadujeme nejen detekci, ale i opravu chyb lineárního kódu, může dekodér pracovat s následující *tabulkou pro opravování chyb*:

$\boldsymbol{o}$	$\boldsymbol{o}$	$\boldsymbol{v}_2$	$\boldsymbol{v}_3$	$\dots$	$\boldsymbol{v}_{2^k}$
$\boldsymbol{s}_2$	$\boldsymbol{e}_2$	$\boldsymbol{e}_2+\boldsymbol{v}_2$	$\boldsymbol{e}_2+\boldsymbol{v}_3$	$\dots$	$\boldsymbol{e}_2+\boldsymbol{v}_{2^k}$
$\boldsymbol{s}_3$	$\boldsymbol{e}_3$	$\boldsymbol{e}_3+\boldsymbol{v}_2$	$\boldsymbol{e}_3+\boldsymbol{v}_3$	$\dots$	$\boldsymbol{e}_3+\boldsymbol{v}_{2^k}$
$\dots$	$\dots$				
$\boldsymbol{s}_{2^{(n-k)}}$	$\boldsymbol{e}_{2^{(n-k)}}$	$\boldsymbol{e}_{2^{(n-k)}}+\boldsymbol{v}_1$	$\boldsymbol{e}_{2^{(n-k)}}+\boldsymbol{v}_2$	$\dots$	$\boldsymbol{e}_{2^{(n-k)}}+\boldsymbol{v}_{2^k}$

Vlevo od svislé čáry jsou syndromy, k těm se vrátím později. Nejprve vysvětlím obsah tabulky vpravo od svislé čáry. Tam jsou rozmístěna všechna slova lineárního prostoru $\mathbf{Z}_2^n$. V prvním řádku jsou kódová slova (je jich 2^k) a v ostatních řádcích jsou slova nekódová. Počet řádků je $2^{(n-k)}$, protože tak získáme celkový počet slov $2^n = 2^k \cdot 2^{(n-k)}$. V prvním sloupci (vpravo od čáry) je nahoře umístěno nulové slovo a pod ním jsou postupně všechna chybová slova, která chceme, aby dekodér uměl odhalit a chybu opravit. Na ostatních pozicích tabulky jsou součty chybového slova v řádku s kódovým slovem ve sloupci.

Tabulku vytvoříme tak, že zapíšeme nejprve do prvního řádku nulové kódové slovo a pak ostatní kódová slova (na pořadí nezáleží). Do druhého řádku napíšeme nejprve chybové slovo, které chceme dekodérem opravovat, a dále příslušné součty. Chybové slovo nesmí být slovem kódovým. Na třetím řádku napíšeme další chybové slovo. Toto chybové slovo se *nesmí*

vyskytovat nikde na předchozích řádcích. K němu do řádku doplníme příslušné součty. Tak postupujeme dále, až vytvoříme tabulku s $2^{(n-k)}$ řádky.

První řádek tabulky obsahuje lineární prostor K, druhý řádek tabulky obsahuje množinu $K+\boldsymbol{e}_2$, která je podle věty ?? disjunktní s K. Platí totiž $\boldsymbol{e}_2 \notin K$. Třetí řádek obsahuje množinu $K + \boldsymbol{e}_3$, která je disjunktní s K i s $K + \boldsymbol{e}_2$, protože $\boldsymbol{e}_3 \notin K$ a $\boldsymbol{e}_3 \notin K + \boldsymbol{e}_2$, takže můžeme dvakrát použít větu ??. A tak dále. Slova v jednom řádku jsou samozřejmě různá. Máme tedy zaručeno, že žádné slovo se v tabulce neopakuje a že jsou vyčerpána všechna slova prostoru $\mathbf{Z}_2^n$.

Pokud nyní dekodér přijme slovo $\boldsymbol{w}$, vyhledá ho v tabulce. Například slovo našel na i-tém řádku tabulky. Dekodér na základě toho rozhodne, že došlo k chybě $\boldsymbol{e}_i$ a opraví ji tak, že provede $\boldsymbol{w} - \boldsymbol{e}_i$. (Místo odčítání může vykonat $\boldsymbol{w} + \boldsymbol{e}_i$, protože v aritmetice $\mathbf{Z}_2$ to dopadne stejně). Pokud $\boldsymbol{w}$ bylo na j-tém sloupci tabulky, dekodér se tímto postupem vrací ke kódovému slovu $\boldsymbol{v}_j$.

Aby dekodér nemusel prohledávat celou tabulku o 2^n slovech, vypočte nejdříve syndrom přijatého vektoru: $\boldsymbol{s}^T = \mathbf{H} \cdot \boldsymbol{w}^T$. Vlevo od svislé čáry jsou syndromy všech slov, které jsou napsány vpravo na stejném řádku (viz věta ??). Prohledáním tabulky syndromů a porovnáním se syndromem slova $\boldsymbol{w}$ dekodér odhalí správně řádek tabulky, ve kterém slovo $\boldsymbol{w}$ leží. Dekodér tedy nemusí pracovat s celou tabulkou, ale jen se sloupcem syndromů a sloupcem chybových slov.

16.54. Příklad. Než se pustíme do formulace požadavků na ideální kód pro opravu chyb, zkusíme sestavit tabulku pro opravování chyb pro případ kódů, kde to nebude příliš užitečné: kód s kontrolním bitem parity a opakovací kód. Tím odhalíme problémy, kterých bychom se měli při návrhu kódů s opravou chyb vyvarovat.

Lineární (4,3) kód s kontrolním bitem parity má například tuto tabulku pro opravování chyb:

0	0000	0011	0101	0110	1001	1010	1100	1111
1	1000	1011	1101	1110	0001	0010	0100	0111

V této tabulce jsme zvolili chybové slovo 1000. Proto dekodér při obdržení nekódového slova opraví první bit. Kdybychom zvolili jiné chybové slovo (např. 0100), dostaneme jinou tabulku: druhý řádek bude obsahovat slova v jiném pořadí. Dekodér podle takové pozměněné tabulky bude po přijetí nekódového slova opravovat jiný bit. Bohužel, nemáme žádnou záruku, že dekodér opraví správný bit. Tabulka určuje pevně jeden bit, který bude dekodér opravovat. Lepší by bylo, kdybychom v prvním sloupci s chybovými slovy měli zapsána všechna chybová slova tvaru 1000, 0100, 0010, 0001. To bychom ale potřebovali mít v tabulce pět řádků a ne jen dva. Dva řádky v tabulce jsou důsledkem toho, že kód pracuje jen s jedním kontrolním bitem a že $2^1 = 2$. Můžeme tedy říci, že pro úspěšnou opravu chyb je jeden kontrolní bit málo. To ostatně člověk intuitivně tuší i bez sestavování tabulek pro opravování chyb.

Lineární (6,3) opakovací kód s kontrolní i generující maticí

$$\mathbf{H} = \mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

může mít například následující tabulku pro opravování chyb:

000	000000	100100	010010	001001	110110	011011	101101	111111
100	100000	000100	110010	101001	010110	111011	001101	011111
010	010000	110100	000010	011001	100110	001011	111101	101111
001	001000	101100	011010	000001	111110	010011	100101	110111
110	110000	010100	100010	111001	000110	101011	011101	001111
101	101000	001100	111010	100001	011110	110011	000101	010111
011	011000	111100	001010	010001	101110	000011	110101	100111
111	111000	011100	101010	110001	001110	100011	010101	000111

Pokud dekodér pracuje podle této tabulky a přijme například slovo 111110, vypočte nejdříve syndrom $\mathbf{H} \cdot (111110)^T = (001)^T$, Dekodér zjistil, že slovo leží ve čtvrtém řádku tabulky. Tam je zvoleno chybové slovo 001000, takže dekodér opraví třetí bit a z přijatého slova 111110 dostává kódové slovo 110110.

Jestliže předpokládáme, že přijaté slovo obsahuje jednu chybu, pak výše uvedená oprava nemusí být jediná možná. Opravou posledního bitu ve slově 111110 také dostáváme kódové slovo 111111. Problém tohoto kódu z pohledu tabulky pro opravování chyb je, že chybová slova s jednou jedničkou se objeví dvě na společném řádku tabulky. Na dalších řádcích (za čtvrtým řádkem) už nemůžeme použít chybové slovo 000001, protože toto slovo se na čtvrtém řádku už objevilo. Pokud bychom na čtvrtém řádku použili chybové slovo 000001, pak by se na tomto řádku zase vyskytlo i 001000. Množina slov vedle konkrétního syndromu se totiž nemůže změnit, protože se jedná o množinu řešení soustavy $\mathbf{H}\boldsymbol{x}^T = \boldsymbol{s}^T$. Takže bychom dostali sice jinou tabulku pro opravování chyb, ale chybová slova s jednou jedničkou by se ani tak nepodařilo oddělit do jednotlivých řádků. Ačkoli (na rozdíl od kódu s kontrolním bitem parity) máme v tabulce dostatečný počet řádků, nemáme možnost dostat všechna chybová slova s jednou jedničkou do prvního sloupce tabulky. Dokonce jsme nuceni na posledním řádku tabulky použít chybové slovo se třemi jedničkami.

16.55. Poznámka. Nezdary při opravování chyb v předchozím příkladě nás inspirují k formulaci podmínek na kód, který spolehlivě opravuje jednu chybu.

Předpokládáme lineární (n, k) kód. Chybových slov s jednou jedničkou je n a potřebujeme je všechna rozmístit do prvního sloupce tabulky pro opravování chyb. Žádná jiná chybová slova se v tomto sloupci nesmějí objevit. Z toho vyplývá, že počet řádků tabulky musí být $n + 1$ (první řádek tabulky obsahuje samotný kód). Protože počet řádků tabulky je $2^{(n-k)}$, máme podmínku $2^{(n-k)} = n+1$. Označíme-li počet kontrolních bitů $c = n-k$, pak je uvedená

podmínka asi lépe čitelná ve tvaru $n = 2^c - 1$. Celkový počet bitů n tedy musí být o jedničku menší než mocnina dvojky a hodnota této mocniny udává počet kontrolních bitů. Postupně pro $c = 2, 3, 4, 5, 6, \ldots$ dostáváme (3,1), (7,4), (15,11), (31,26), (63,57), ... kódy.

Abychom mohli rozmístit všechna chybová slova s jednou jedničkou do prvního sloupce, potřebujeme ještě zaručit, že žádné slovo s jednou jedničkou není kódové slovo a že dvě slova s jednou jedničkou nebudou mít stejný syndrom. Tuto podmínku nejlépe charakterizuje následující věta.

16.56. Věta. Slovo s jednou jedničkou je kódové právě tehdy, když kontrolní matice obsahuje nulový sloupec. Dvě různá slova s jednou jedničkou mají společný syndrom právě tehdy, když kontrolní matice obsahuje aspoň dva stejné sloupce.

Důkaz. Stačí si uvědomit, že syndrom slova s jednou jedničkou na i-tém místě je roven i-tému sloupci kontrolní matice. To vyplývá z maticového násobení $\mathbf{H} \cdot \boldsymbol{w}^T = \boldsymbol{s}^T$.

16.57. Poznámka. Aby lineární (n, k) kód opravoval všechny jednoduché chyby ve slově, je podle poznámky ?? nutné, aby $n = 2^c - 1$, kde $c = n - k$, a dále podle věty ?? je nutné, aby kontrolní matice neměla žádný sloupec nulový a všechny sloupce od sebe vzájemně různé. Těch sloupců musí být $n = 2^c - 1$, a přitom výška sloupce je c. Z toho nám vyplývá jediný možný tvar kontrolní matice (až na pořadí sloupců): v jednotlivých sloupcích kontrolní matice napíšeme ve dvojkové soustavě všechna čísla $1, 2, 3, \ldots, n$. Lineárnímu kódu s takovou kontrolní maticí říkáme *Hammingův kód*.

16.58. Příklad. Ukážeme si Hammingův $(7, 4)$ kód. Podle předchozí poznámky napíšeme ve dvojkové soustavě do sloupců kontrolní matice čísla 1,2,3,4,5,6,7:

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

Syndromy a první sloupec tabulky pro opravování chyb napíšeme (kvůli úspoře místa v tomto textu) místo do sloupců do řádků:

000	001	010	011	100	101	110	111
0000000	1000000	0100000	0010000	0001000	0000100	0000010	00000001

Vidíme, že při této volbě pořadí sloupců kontrolní matice má dekodér výrazně usnadněnou práci: nemusí prohledávat v tabulce syndromů, aby zjistil odpovídající chybové slovo. Stačí, aby interpretoval syndrom jako číslo zapsané ve dvojkové soustavě. Toto číslo udává pozici bitu chybového slova, kde se nalézá jednička.

Jak tedy bude dekodér postupovat při obdržení slova $\boldsymbol{w}$? Vypočte syndrom pomocí $\boldsymbol{s}^T = \mathbf{H} \cdot \boldsymbol{w}^T$ a interpretuje jej jako číslo i ve dvojkové soustavě. Je-li $i = 0$, je $\boldsymbol{w}$ kódové slovo a dekodér nic neopravuje. Je-li $i > 0$, pak dekodér opraví v obdrženém slově i-tý bit.

Tím je kompletně navržen dekodér Hammingova $(7,4)$ kódu a zbývá ještě navrhnout kodér. Eliminací kontrolní matice přecházíme ke kontrolní matici stejného kódu (poznámka ??):

$$\mathbf{H} = \begin{pmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \end{pmatrix} \sim \begin{pmatrix} 1&0&1&1&0&1&0 \\ 1&1&0&0&1&1&0 \\ 1&0&1&0&1&0&1 \end{pmatrix} \sim \begin{pmatrix} 0&1&1&1&1&0&0 \\ 1&1&0&0&1&1&0 \\ 1&0&1&0&1&0&1 \end{pmatrix} \sim \begin{pmatrix} 0&1&1&1&1&0&0 \\ 1&0&1&1&0&1&0 \\ 1&1&0&1&0&0&1 \end{pmatrix} =$$

Podle věty ?? se tedy jedná o systematický kód, protože $\mathbf{H}' = (\mathbf{C}^T|\mathbf{E}')$. Podle poznámky ?? nyní přejdeme ke generující matici $\mathbf{G} = (\mathbf{E}|\mathbf{C})$:

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

Kodér necháme nejprve kopírovat první čtyři informační bity do výstupu a další tři kontrolní bity $\boldsymbol{v}'$ počítáme ze vstupního slova $\boldsymbol{u}$ podle poznámky ??:

$$\boldsymbol{v}' = \boldsymbol{u} \cdot \begin{pmatrix} 0&1&1 \\ 1&0&1 \\ 1&1&0 \\ 1&1&1 \end{pmatrix}.$$

16.59. Poznámka. Analogicky se postupuje při návrhu $(15, 11)$, $(31, 26)$, $(63, 57)$ atd. Hammingových kódů. Všimněte si, že s rostoucím n se výrazně zlepšuje poměr informačních bitů ku celkovému počtu přenášených bitů. To je pro uživatele, kteří se zajímají jen o informační bity, dobrá zpráva. Ovšem prodlužováním délky přenášených slov se zase zvyšuje pravděpodobnost výskytu více než jedné chyby ve slově. Dekodér Hammingova kódu v takovém případě selže.

16.60. Poznámka. Ve výpočetní technice se pracuje s přenosy 8 bitů, 16 bitů, 32 bitů atd. Hammingův kód předpokládá přenos slov délky o jeden bit kratší. Co se zbylým bitem? Použijeme jej pro kontrolu parity. Tím dostáváme *rozšířený Hammingův kód*, který umožní spolehlivě opravit jednu chybu a detekovat chyby dvě.

16.61. Příklad. K Hammingovu kódu $(7, 4)$ přidáme kontrolní bit parity a dostáváme lineární $(8, 4)$ kód s následující kontrolní maticí:

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

Tento kód umí opravit jednu chybu ve slově a detekovat chyby dvě. Jak dekodér může postupovat? Přijme slovo $\boldsymbol{w}$ a vypočte syndrom $\boldsymbol{s}^T = \mathbf{H} \cdot \boldsymbol{w}^T$. Je-li syndrom nulový vektor, je

slovo $\boldsymbol{w}$ kódové a dekodér nic neopravuje. Jsou-li první tři bity syndromu nulové a poslední nenulový, došlo při přenosu jen k chybě posledního kontrolního bitu parity. Je-li na prvních třech pozicích syndromu aspoň jeden bit nenulový a poslední bit syndromu je rovněž nenulový, došlo k lichému počtu chyb ve slově. Dekodér předpokládá, že došlo k jediné chybě a podle prvních třech bitů syndromu zjistí, který bit ve slově má opravit (stejně jako v příkladu ??). Je-li konečně poslední bit syndromu nulový, ale syndrom obsahuje aspoň jeden nenulový bit, pak došlo k sudému počtu chyb. Tento počet chyb neumí dekodér opravit, ale detekuje tento stav jako dvojnásobnou chybu.

16.62. Poznámka. Všimněte si, že nejmenší Hammingova vzdálenost mezi dvěma slovy rozšířeného Hammingova kódu je 4. To je v souladu s výsledky příkladu ??.

17. Literatura

[1] J. Adámek, *Foundations of Coding.* A Wiley-Interscience publication, New York 1991.

[2] V. Bartík, *Úvod do algebry.* Text k přednášce 1996 na http://math.feld.cvut.cz/bartik/

[3] H.–J. Bartsch, *Matematické vzorce.* Academia, Praha 2006 (4. vydání).

[4] R. A. Beezer, *A First Course in Linear Algebra.* Tacoma, Washington, USA 2007. Text je mj. volně dostupný na http://linear.ups.edu/.

[5] L. Bican, *Lineární algebra a geometrie.* Academia, Praha 2002.

[6] G. Birkhoff, S. MacLane, *Algebra.* Chelsea Pub Co, (3rd edition) 1993. Existuje slovenský překlad staršího vydání *Prehľad modernej algebry*, Alfa, Bratislava, 1979.

[7] Don Coppersmith and Shmuel Winograd. *Matrix multiplication via arithmetic progressions.* Journal of Symbolic Computation, 9:251?280, 1990.

[8] M. Demlová, B. Pondělíček, *Úvod do algebry.* Vydavatelství ČVUT, Praha 1996.

[9] M. Dont, *Elementy numerické lineární algebry.* Vydavatelství ČVUT, Praha 2004.

[10] I. M. Gelfand, *Lineární algebra.* Překlad M. Fiedler, ČSAV, Praha 1953.

[11] J. Hefferon, *Linear Algebra.* Colchester, Vermont USA, volně dostupné na http://joshua.smcvt.edu/linearalgebra/.

[12] S. Jílková, V. Maňasová, Z. Tischerová, *Lineární algebra – úlohy.* Vydavatelství ČVUT, Praha 1987.

[13] A. Kalousová, *Skripta z algebry.* Text volně dostupný například z ftp://math.feld.cvut.cz/pub/kalous/Skripta/skripta.pdf

[14] T. Kepka, *Algebra.* Poznámky z přednášek na MFF UK dostupné např. na http://lucy.troja.mff.cuni.cz/labtf/poznamky/.

[15] V. Kořínek, *Základy algebry.* Klasická učebnice algebry, Academia, Praha 1956 (2. vydání).

[16] E. Krajník, *Základy maticového počtu.* Vydavatelství ČVUT, Praha 2006.

[17] V. Mahel & kol. kat. matematiky, *Sbírka úloh z lineární algebry a analytické geometrie.* Vydavatelství ČVUT, Praha 1986.

[18] J. Matoušek, *Šestnáct miniatur.* Volně dostupný text s aplikacemi lineární algebry tam, kde bychom to možná nečekali, http://kam.mff.cuni.cz/~matousek/la1.html.

[19] L. Motl, M. Zahradník, *Pěstujeme lineární algebru.* MFF UK, Praha 1994 (skriptum přístupné na http://www.kolej.mff.cuni.cz/~lmotm275/skripta/).

[20] P. Olšák, *Úvod do algebry, zejména lineární.* FEL ČVUT, Praha 2007.

[21] P. Olšák, *TEXbook naruby.* Konvoj, Brno 2001 (2. vydání). Text volně dostupný například na http://petr.olsak.net/tbn.html.

[22] L. Procházka, *Algebra.* Academia, Praha 1990.

[23] I. V. Proskurjakov, *Sbornik zadač po linějnoj algebre.* Uzdavatělstvo Nauka, Moskva 1970.

[24] P. Pták, *Introduction to Linear Algebra.* Vydavatelství ČVUT, Praha 2006.

[25] K. Rektorys, *Přehled užité matematiky.* Prometheus, Praha 2003 (6. vydání).

[26] P. Vopěnka, *Úhelný kámen evropské vzdělanosti a moci – rozpravy s geometrií.* Práh, Praha 2003.

[27] K. Výborný, M. Zahradník & kol. *Sbírka příkladů z lineární algebry.* Volně dostupný text k nalezení například na http://www.kolej.mff.cuni.cz/~lmotm275/skripta/.

[28] J. Žára, B. Beneš, J. Sochor, P. Felkel, *Moderní počítačová grafika.* Computer Press, 2005 (2. vydání).