=-20mm

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: 20. 6. 2017 (beta verze druhého vydání)

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

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

V roce 2010 jsem začal pracovat na „druhém vydání“ tohoto textu, který se
razně liší od předchozího. V některých partiích jsem začal používat (domní
se) užitečnější značení, ale především jsem text rozčlenil do kapitol výra
jiným způsobem a opustil jsem od zpětné kompatibility číslování odstav
první verzí. Druhé vydání má zdrojový soubor `linal2.tex`.
K teoretickému úvodu (lineární prostor, lineární závislost, obaly, báze) př
vám pojem souřadnice vzhledem k bázi a v následující kapitole o zobraze
ukážu, že souřadnice vzhledem k bázi jsou izomorfismem na $\mathbf{R}^n$. Tím

algoritmus, geometrická interpretace množiny řešení soustavy rovnic, ma
afinního zobrazení v homogenních souřadnicích. Na konec každé kapitoly j
připojil odstavec „shrnutí“, který lapidárním jazykem shrnuje, co bylo v k
tole řečeno.

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

Obsah

Gaussova eliminační metoda

Než se pustíme do studia lineárních prostorů a podprostorů, závislos
nezávislosti vektorů, bází a lineárních obalů, uvedeme si v této úvodní kapi
metodu, která se nám bude často hodit. Protože se k řešení soustav vrát
podrobněji v kapitole devíté, řekneme si zde jen to nejnutnější a budem
v některých případech vyjadřovat možná poněkud těžkopádně. Vše naprav
v deváté kapitole.

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

Metodu si nejprve vysvětlíme na jednoduchém příkladě následující
stavy 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 postupn
dosazením, nebo násobením rovnic konstantami a vzájemným sčítáním rov
Metoda postupného dosazení by mohla vypadat takto:

$$2x - 5y = 16 \quad \Rightarrow \quad 2(2y + 7) - 5y = 14 - y = 16 \quad \Rightarrow \quad \underline{y}$$

(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 které je již řešení snadno čitelné. Jednotlivé modifikace naší soustavy od oddělujeme znakem „$\sim$“.

$$\begin{aligned} 2x - 5y &= 16 \\ -x + 2y &= -7 \end{aligned} \sim \begin{aligned} 2x - 5y &= 16 \\ -2x + 4y &= -14 \end{aligned} \sim \begin{aligned} 2x - 5y &= 16 \\ 0x - y &= 2 \end{aligned} \sim \begin{aligned} 2x - 5y &= 16 \\ y &= -2 \end{aligned}$$

Nejprve jsme vynásobili druhou rovnici dvěma, pak jsme obě rovnice seče výsledek napsali na místo druhé rovnice, dále jsme druhou rovnici vynás číslem -1, pak jsme pětinásobek druhé rovnice přičetli k první a nakonec j první rovnici vynásobili číslem $1/2$. Z poslední soustavy čteme přímo řeše

Gaussova eliminační metoda je vlastně shodná s právě použitou meto „sčítání rovnic“. Navíc Gaussova metoda upřesňuje postup, jak rovnice nás a sčítat mezi sebou, abychom se cíleně dobrali k výsledku i u rozsáhlých sou mnoha rovnic s mnoha neznámými. Než tento postup popíšeme, zamyslím nad tím, jak stručně můžeme soustavy rovnic zapisovat. V soustavě rovnic při hledání řešení podstatné, zda se neznámé jmenují x, y, z nebo třeba $\alpha,$ Podstatné jsou jen koeficienty, které násobí jednotlivé neznámé, a samozře ještě hodnoty na pravých stranách rovnic. Oddělíme tedy „zrno od ple vypíšeme z naší soustavy jen to podstatné (koeficienty u neznámých a hod 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 řá

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

Máme řešit následující soustavu lineárních rovnic

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

Koeficienty této soustavy přepíšeme do matice a matici budeme upravovat
mocí tzv. kroků Gaussovy eliminační metody, mezi které patří prohození řá
mezi sebou, vynásobení řádku nenulovou konstantou nebo přičtení libovoln
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 náso
dostat nulu pod první prvek v prvn
Aby se nám to lépe dělalo, prohodím
dek s druhým.

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

Pod dvojkou v prvním sloupci budem
vytvářet nuly. Vezmeme dvojnásob

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

Nyní bychom měli vytvářet nuly ve d
To se v tomto případě stalo (výjime
takže se zaměříme na třetí sloupec
první jedničkou v druhém řádku vytv
takto: minus trojnásobek druhého
čteme ke třetímu a dále druhý řáde
ke čtvrtému. První a druhý řádek o

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

Znovu se přesuneme na další sloupec
čtvrtý) a vytvoříme nulu pod minus
třetího řádku. K tomu stačí sečíst
se čtvrtým a výsledek napsat na mís
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) v
číslem $-1/2$. Čtvrtý řádek nemusíme
tože tento řádek odpovídá rovnici 0
$0x_3 + 0x_4 + 0x_5 = 0$, která je zřej
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
ve svém „dolním levém koutě“ nul
každý další řádek má zleva aspoň o
více než předešlý. To je cílem tzv. *pří*
Gaussovy eliminační metody, který
ukončili.

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

tři neznámé. Pomocí poslední rovnice budeme počítat například x_4, pom
předposlední rovnice budeme počítat x_3 a z první rovnice spočítáme napří
x_1. Ostatní neznámé nejsou těmito rovnicemi určeny a mohou nabývat libo
ných hodnot. To dáme najevo například takto: $x_5 = u$, $x_2 = v$, $u \in \mathbf{R}$, $v \in$
Nyní budeme počítat hodnoty ostatních neznámých dosazovací metodou,
stupujeme od poslední rovnice k první:

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

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

Pokud bychom se rozhodli například z první rovnice počítat x_2, pak
neznámá x_1 mohla nabývat libovolných hodnot a výsledek by byl form
zapsán poněkud jinak: $x_1 = w$, $x_2 = -8 + 2u + 2w$, $x_3 = -4 - u$, $x_4 = 1 +$
$x_5 = u$, $u \in \mathbf{R}$, $w \in \mathbf{R}$. Vidíme tedy, že neexistuje jednoznačný zápis výsle

v s-tém sloupci pod nenulovým prvkem matice v r-tém řádku. Názorně:

$$
\begin{array}{r}
\\ \\ \\ \\ \\ \text{ádek } r \rightarrow \\ \\ \\ \\ \\
\end{array}
\begin{array}{c}
\begin{array}{cccccc} & & & \text{sloupec } s & & \\ & & & \downarrow & & \end{array} \\
\left(\begin{array}{cccccc|c}
\bullet & \cdots & \bullet & \bullet & \bullet & \cdots & \bullet \\
 & \vdots & & & & \vdots & \bullet \\
0 & \cdots & 0 & a & \bullet & \cdots & \bullet \\
0 & \cdots & 0 & b_1 & \bullet & \cdots & \bullet \\
 & \vdots & & \vdots & & \vdots & \\
0 & \cdots & 0 & b_k & \bullet & \cdots & \bullet
\end{array}\right)
\end{array}
\sim
\begin{array}{c}
\begin{array}{cccccc} & & & \text{sloupec } s & & \\ & & & \downarrow & & \end{array} \\
\left(\begin{array}{cccccc|c}
\bullet & \cdots & \bullet & \bullet & \bullet & \cdots & \bullet \\
 & \vdots & & & & \vdots & \bullet \\
0 & \cdots & 0 & a & \bullet & \cdots & \bullet \\
0 & \cdots & 0 & 0 & \bullet & \cdots & \bullet \\
 & \vdots & & \vdots & & \vdots & \\
0 & \cdots & 0 & 0 & \bullet & \cdots & \bullet
\end{array}\right)
\end{array}
\leftarrow
$$

Tečkami jsou v tomto obrázku vyznačeny prvky matice, jejichž hodnoty momentálně nezajímají. Prvek a musí být nenulový. Procedura „vytvoření 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 $r+2$ přičít $(-b_2/a)$ násobek řádku r, atd., až konečně k řádku poslednímu přičít $(-b_k/a)$ násobek řádku r.

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

Nyní popíšeme přímý chod Gaussovy eliminační metody, který přev libovolnou matici na schodovitou matici, která má „v levém dolním rohu“ n Matice bude mít v každém řádku zleva aspoň o jednu nulu více v souvislé nul, než v předchozím řádku. V algoritmu se pracuje s proměnnou r označ aktuální řádek a s proměnnou s, která znamená sloupec, ve kterém v da okamžiku vytváříme nuly. Pokud se v algoritmu zvětšuje r, a přitom r označuje poslední řádek matice, ukončíme činnost. Pokud by se mělo zvě

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

G4. Vytvoříme nuly pod nenulovým prvkem a z r-tého řádku a s-tého slo
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
znova.

Při eliminační metodě jsme převedli matici koeficientů soustavy na ji
matici odpovídající jiné soustavě, ale se stejnou množinou řešení, protože
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 odp
dající nové soustavě se stejnou množinou řešení. Stačí se tedy zaměřit na
novou soustavu. Nejprve rozhodneme, zda soustava má vůbec nějaké ře
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 sousta soustava může mít podstatně více rovnic než neznámých, ale po eliminaci takovém případě zákonitě počet rovnic zmenší.

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

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

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

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

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

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

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

V úpravě (1) jsme vytvořili nuly pod jedničkou z prvního sloupce a prv
řádku. V úpravě (2) jsme přehodili druhý řádek se čtvrtým v souladu s
kem G3 našeho algoritmu (na druhém řádku a druhém sloupci totiž byl nu
prvek). V úpravě (3) jsme vytvořili nuly pod jedničkou z druhého řádku v
hém sloupci. V poslední úpravě (4) jsme vytvořili nulu pod jedničkou v tř
sloupci z třetího řádku. Tím máme matici v požadovaném tvaru. Pohleden
poslední řádek okamžitě vidíme, že soustava nemá řešení.

1. Lineární prostor

[dvd] *O formě definice-věta-důkaz.* V tomto textu narazíte na tři zákla „slohové útvary“: definice, věta a důkaz. Vesměs každé solidní matemat sdělení používá tyto pojmy. Přitom je možné, že s takto systematickým užitím pojmů definice, věta, důkaz se setkáváte poprvé. Proto si tyto po vysvětlíme.

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

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

Důkaz je obhajoba platnosti věty. Při této obhajobě můžeme použít p chozí definice (zaměníme použitý pojem ve větě skupinou pojmů, kterým pojem definován) a dále můžeme použít dříve dokázané věty (ověříme p poklady dříve dokázané věty a použijeme pak její vlastní tvrzení). Dál v důkazech používá logických obratů, které byste měli znát ze střední š exaktní.

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

V následující definici lineárního prostoru ?? se pracuje s množinami nespecifikovaných objektů. Jediné, co s těmi objekty umíme dělat, je vzáje objekty sčítat a násobit objekt reálným číslem. Přitom tyto operace (sčítá násobení reálným číslem) je potřeba pro konkrétní množiny objektů defino Pro každou množinu objektů mohou tyto operace vypadat jinak. Skutečn že není řečeno, jak objekty a operace s nimi konkrétně vypadají, může pro některé čtenáře poněkud frustrující. Proto před definicí uvedeme přík množin objektů, které lze sčítat a násobit konstantou.

[dvojice] Nechť $\mathbf{R}^2$ je množina všech uspořádaných dvojic reálných č Uspořádanou dvojici zapisujeme ve tvaru (a, b). Vyznačujeme ji tedy kul závorkou a její složky a, b píšeme odděleny čárkou. Takže $\mathbf{R}^2 = \{(a, b);\ a \in$ $b \in \mathbf{R}\}$. Symbol $\mathbf{R}$ značí reálná čísla a zápisem $\{X;\ \text{vlastnost } X\}$ zna množinu objektů X, které mají specifikovanou vlastnost. Definujme sč dvou uspořádaných dvojic:

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

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

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

Všimneme si, že jsme definovali operaci $\oplus$ sčítání objektů tak, že výsle sčítání je zase uspořádaná dvojice. Stejně součin $\odot$ reálného čísla s uspořáda

Všimneme si dále, že jsme definovali nové operace $\oplus$ a $\odot$ prostřednict
operací sčítání a násobení reálných čísel, tj. prostřednicvím operací, jej
vlastnosti jsou známy ze střední školy. Příkladem takové vlastnosti je kom
tivní zákon (pro reálná čísla x a y platí: $x + y = y + x$). Naše nově definov
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 $(c, d) \oplus (a, b) = (c+a, d$
ovšem dvě uspořádané dvojice se rovnají, pokud se rovnají odpovídající slo
V tomto případě první složka první dvojice $a + b$ se rovná první složce dr
dvojice $b + a$, neboť pro sčítání reálných čísel platí komutativní zákon. Podo
ověříme i druhou složku.

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

$$(a, b) \underline{\oplus} (c, d) \stackrel{\mathrm{df}}{=} (2a + d, b + c), (plusdvojicejinak)$$

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

[polynomy] Označme P množinu všech reálných polynomů, tedy fu
$p : \mathbf{R} \to \mathbf{R}$, které pro $x \in \mathbf{R}$ mají hodnotu danou vzorcem:

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

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

hodnoty funkce q v bodě x. Tyto hodnoty jsou reálná čísla, takže sčítání fu (nové sčítání nových objektů) vlastně definujeme pomocí sčítání reálných (sčítání, které známe ze střední školy). Podobně definujeme násobek fu reálným číslem.

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

[pretezovani] V předchozích dvou příkladech jsme definovali na mno nějakých objektů sčítání a násobení reálným číslem. Pro větší přehlednost j nově definované operace zapisovali do kroužku, abychom je odlišili od ope sčítání a násobení reálných čísel. To ale není potřeba. Stačí používat t znaky, protože podle typu objektů, které do operace vstupují, okamžitě známe, jakou operaci máme použít (zda nově definovanou nebo známou ope na reálných číslech). Takové automatické přizpůsobení operace podle typu randů znají programátoři objektově orientovaných jazyků. Tam se tomu „přetěžování operátorů".

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

V dalším textu budeme skoro vždy používat znaky „+" a „·" i pro definované operace, protože podle typu operandů nemůže dojít k nedor mění. Také znak násobení „·" budeme někdy vynechávat, jako jsme zvykl vynechávat při zápisu násobení reálných čísel.

* [dlp] *Lineárním prostorem* nazýváme každou neprázdnou množinu L které je definováno sčítání $+ : L \times L \to L$ a násobení reálným číslem $\cdot : \mathbf{R} \times$ L a tyto operace splňují pro každé $\boldsymbol{x} \in L, \boldsymbol{y} \in L, \boldsymbol{z} \in L, \alpha \in \mathbf{R}, \beta \in \mathbf{R}$ vlastn

(1) $\boldsymbol{x} + \boldsymbol{y} = \boldsymbol{y} + \boldsymbol{x}$ (komutativní zá

(2) $(\boldsymbol{x} + \boldsymbol{y}) + \boldsymbol{z} = \boldsymbol{x} + (\boldsymbol{y} + \boldsymbol{z})$ (asociativní zák

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

[nulprvek] Pro nulový prvek $\boldsymbol{o}$ lineárního prostoru L platí vlastnosti:

$$
\begin{aligned}
&(1) \quad \boldsymbol{x} + \boldsymbol{o} = \boldsymbol{x} \qquad \forall\, \boldsymbol{x} \in L,\\
&(2) \quad \alpha \cdot \boldsymbol{o} = \boldsymbol{o} \qquad \forall\, \alpha \in \mathbf{R},\\
&(3) \quad \text{Nechť } \boldsymbol{x} \in L. \quad \text{Je-li} \quad \alpha \cdot \boldsymbol{x} = \boldsymbol{o} \quad \text{a} \quad \alpha \neq 0, \quad \text{pak} \quad \boldsymbol{x} = \boldsymbol{o}.
\end{aligned}
$$

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

$$
\begin{aligned}
&(1) \quad \boldsymbol{x} + \boldsymbol{o} \overset{(7)}{=} \boldsymbol{x} + 0 \cdot \boldsymbol{x} \overset{(6)}{=} 1 \cdot \boldsymbol{x} + 0 \cdot \boldsymbol{x} \overset{(5)}{=} (1+0) \cdot \boldsymbol{x} = 1 \cdot \boldsymbol{x} \overset{(6)}{=} \boldsymbol{x}.\\
&(2) \quad \alpha \cdot \boldsymbol{o} \overset{(7)}{=} \alpha \cdot (0 \cdot \boldsymbol{x}) \overset{(3)}{=} (\alpha \cdot 0) \cdot \boldsymbol{x} = 0 \cdot \boldsymbol{x} \overset{(7)}{=} \boldsymbol{o}.\\
&(3) \quad \boldsymbol{x} \overset{(6)}{=} 1 \cdot \boldsymbol{x} = \left(\frac{1}{\alpha}\alpha\right) \cdot \boldsymbol{x} \overset{(3)}{=} \frac{1}{\alpha} \cdot (\alpha \cdot \boldsymbol{x}) \overset{\text{(z předpokladu)}}{=} \frac{1}{\alpha} \cdot \boldsymbol{o} \overset{\text{(vlastnost (2) v}}{=}
\end{aligned}
$$

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

Protože lineární prostor obsahuje vektory, v literatuře se často setkáv
s pojmem *vektorový prostor*, který je použit v naprosto stejném smyslu,
zde používáme pojem *lineární prostor*. Je třeba si uvědomit, že *vektory* v to

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

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

$$\big((a,b)+(c,d)\big)+(e,f) = (a+c,b+d)+(e,f) = \big((a+c)+e,(b+d)+f\big)$$
$$= \big(a+(c+e),b+(d+f)\big) = (a,b)+(c+e,d+f$$

Při úpravách jsme nejprve dvakrát použili definici (??), pak jsme v jednotliv složkách využili toho, že pro sčítání reálných čísel platí asociativní záko konečně jsme zase dvakrát použili definici (??). Nyní dokážeme další vlastno Pro každé $a, b, c, d, \alpha, \beta \in \mathbf{R}$ platí:

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

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

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

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

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

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

Vidíme, že nulovým vektorem lineárního prostoru $\mathbf{R}^2$ je dvojice (0 Podle konvence ze závěru definice ?? jsme oprávněni uspořádaným dvojicím

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

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

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

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

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

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

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

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

Definujme nyní sčítání $+ : U_O \times U_O \to U_O$ ryze konstruktivně takto: Úse
$\boldsymbol{u} \in U_O$, $\boldsymbol{v} \in U_O$ doplníme na rovnoběžník. Úhlopříčku, která začíná v b
O a končí v protějším bodě rovnoběžníka, prohlásíme za součet úseček $\boldsymbol{u}$
tedy $\boldsymbol{u} + \boldsymbol{v}$. Dále definujme násobení skalárem $\cdot : \mathbf{R} \times U_O \to U_O$ takto: Úseč

orientovaná úsečka a α násobek orientované úsečky je orientovaná úsečka. J
ověříme vlastnosti (1) až (7) z definice ??. (1) $\boldsymbol{u} + \boldsymbol{v} = \boldsymbol{v} + \boldsymbol{u}$, protože v o
případech doplňujeme na stejný rovnoběžník. (2) $(\boldsymbol{u} + \boldsymbol{v}) + \boldsymbol{w} = \boldsymbol{u} + (\boldsymbol{v} +$
protože postupné doplnění úhlopříčky rovnoběžníku $\boldsymbol{u}, \boldsymbol{v}$ a úsečky $\boldsymbol{w}$ na
noběžník vede ke stejnému výsledku, jako když nejprve sestavíme úhlopř
rovnoběžníku $\boldsymbol{v}, \boldsymbol{w}$ a tu doplníme na rovnoběžník s úsečkou $\boldsymbol{u}$ (udělejt
náčtrek). Výsledný součet je tělesová úhlopříčka rovnoběžnostěnu, který je
mezen úsečkami $\boldsymbol{u}$, $\boldsymbol{v}$ a $\boldsymbol{w}$. (3) $\alpha \cdot (\beta \boldsymbol{u}) = (\alpha \beta) \cdot \boldsymbol{u}$, protože na levé st
rovnosti se pracuje s měřítkem, které je βkrát větší než původní měřítko.
původním měřítku se hledá bod $\alpha\beta$ a na βkrát větším měřítku se hledá
α. (4) $\alpha \cdot (\boldsymbol{u} + \boldsymbol{v}) = \alpha \cdot \boldsymbol{u} + \alpha \cdot \boldsymbol{v}$, protože příslušné rovnoběžníky pro sčí
jsou podobné a druhý je α krát větší než první. Proto též jeho úhlopříčka b
α krát větší. (5) $(\alpha + \beta) \cdot \boldsymbol{u} = \alpha \cdot \boldsymbol{u} + \beta \cdot \boldsymbol{u}$, protože sečtení vektorů $\alpha \cdot \boldsymbol{u} +$
probíhá v „degenerovaném" rovnoběžníku, který se celý vejde do přímky.
ní se sčítají úsečky o velikostech α a β, takže dostáváme na měřítku bod α
(6) $1 \cdot \boldsymbol{u} = \boldsymbol{u}$, protože jednička na měřítku leží v koncovém bodě vektoru
(7) $0 \cdot \boldsymbol{u}$ je vždy úsečka kočící v bodě O, protože tam je nula pomysl
měřítka. Degenerovaná úsečka začínající i končící v bodě O je tedy nulo
prvkem našeho lineárního prostoru.

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

[LPfunkci] Uvažujme množinu F_D všech reálných funkcí reálné promě
definovaných na nějaké množině $D \subseteq \mathbf{R}$, tj. $F_D = \{f;\ f : D \to \mathbf{R}\}$. Pro l
volné funkce $f \in F_D$, $g \in F_D$ a pro libovolné reálné číslo α definujme so
$f + g$ a násobek skalárem $\alpha \cdot f$ takto:

$$(f + g)(x) \overset{\text{df}}{=} f(x) + g(x) \quad \forall x \in D \quad (\text{d}$$

funkcí ani násobením funkce konstantou podle naší definice se nemění defin obor a výsledkem operací je znovu reálná funkce reálné proměnné.

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

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

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

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

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

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

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

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

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

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

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

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

F_D, o němž jsme dokázali v příkladu ??, že se jedná o lineární prostor (vo
$D = \mathbf{R}$). Při ověřování vlastností (1) až (7) bychom dělali vlastně to samé
v příkladu ??, jen na podmnožině $P \subseteq F_D$.

[NeLPpolynomu] Nechť $n \in \mathbf{N}$, $n \geq 0$ (symbolem $\mathbf{N}$ značíme množinu
rozených čísel). Množina P_n všech polynomů právě n-tého stupně s definic
sčítání a násobení skalárem podle příkladu ?? *netvoří* lineární prostor. Př
meneme, že *stupeň polynomu* se definuje jako největší $k \in \mathbf{N}$ takové, že a
ve vzorci (??) nenulové. Jsou-li všechna a_k nulová, definujeme stupeň takov
polynomu jako -1.

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

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

[dlpp] Nechť L je lineární prostor s operacemi „+“ a „·“. Neprázd
množinu $M \subseteq L$ nazýváme *lineárním podprostorem prostoru L*, pokud
všechna $\boldsymbol{x} \in M, \boldsymbol{y} \in M$ a $\alpha \in \mathbf{R}$ platí:

$$(1) \quad \boldsymbol{x} + \boldsymbol{y} \in M,$$

$$(2) \quad \alpha \cdot \boldsymbol{x} \in M.$$

reálných funkcí F_D. Je to dáno tím, že (1) součtem polynomů nejvýše n-
stupně dostáváme polynom nejvýše n-tého stupně a (2) vynásobením polyn
nejvýše n-tého stupně reálným číslem dostaneme zase polynom nejvýše n-
stupně.

[LPPRn] Uvažujme $M \subseteq \mathbf{R}^n$, $M = \{(a, a, \ldots, a);\ a \in \mathbf{R}\}$. Předpo
dáme tedy, že množina M obsahuje takové n-tice, ve kterých se všechny slo
vzájemně rovnají. Ukážeme, že M je lineární podprostor lineárního pros
$\mathbf{R}^n$.

Stačí pro množinu M dokázat vlastnosti (1) a (2) z definice ??.
(1) součet dvou uspořádaných n-tic, ve kterých se složky rovnají, je usp
daná n-tice, ve kterých se složky rovnají. (2) vynásobením uspořádané n-
ve které se složky rovnají, reálným číslem, dostáváme zase uspořádanou n-
ve které se složky rovnají.

[LPPR3] Uvažujme množiny $M \subseteq \mathbf{R}^3$, $N \subseteq \mathbf{R}^3$ a $S \subseteq \mathbf{R}^3$, které
definovány takto:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[ObskurniLP] Ukážeme si jeden příklad poněkud exotického lineárního
storu. Jedná se o množinu kladných reálných čísel $\mathbf{R}^+$, na které je definov
„sčítání“ $\oplus : \mathbf{R}^+ \times \mathbf{R}^+ \to \mathbf{R}^+$ a „násobení“ reálným číslem $\odot : \mathbf{R} \times \mathbf{R}^+ \to$
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 „$\cdot$“ je míněno běžné násobení reálných čísel a x^α je reálná moc
o kladném základu.

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

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

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

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

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

[dlpnadC] V definici ?? jsme za skaláry považovali reálná čísla. Nyní
síme nahradit v této definici všechny výskyty množiny **R** množinou komp
ních čísel **C**. Dostáváme pozměněnou definici:

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

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

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

V kapitole patnácté se setkáme s dalším zobecněním lineárního prost
Lineární prostor nad reálnými nebo nad komplexními čísly nahradíme lineár
prostorem nad obecným *tělesem*. Vesměs všechny vlastnosti, které dokáž
pro lineární prostory nad **R**, zůstanou v platnosti i pro lineární prostory
obecným tělesem.

V lineární algebře se pracuje s lineárními prostory /??/, což jsou mno vyklými operacemi, které přesto splňují axiomy linearity /??/.

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

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

2. Lineární závislost a nezávislost, lineární obal

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

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

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

se často vektory zvýrazňují zápisem šipky nad písmeno, podtržením písm
nebo i jinak.

[lk] Nechť $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou vektory (tj. prvky nějakého lineárního storu). *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 *koefici* lineární kombinace.

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

[trivlk] *Triviální* lineární kombinace vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ je taková l ární kombinace, která má všechny koeficienty nulové, tj. $0\boldsymbol{x}_1 + 0\boldsymbol{x}_2 + \cdots + 0$ *Netriviální* lineární kombinace je taková lineární kombinace, která není t ální, tj. aspoň jeden její koeficient je nenulový.

Triviální lineární kombinace je vždy rovna nulovému vektoru.

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

* [LZskupiny] Skupinu vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ nazýváme *lineárně závis* pokud existuje netriviální lineární kombinace vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$, kter rovna nulovému vektoru. Stručně říkáme, že vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou *l árně závislé*.

[poznlz] Pokud bychom rozvedli pojem netriviální lineární kombinace p definic ?? a ??, můžeme říci, že vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou *lineárně záv* pokud existují reálná čísla $\alpha_1, \alpha_2, \ldots, \alpha_n$ tak, že aspoň jedno z nich je nenul a přitom platí

vektoru. Jinak řečeno, jedině triviální lineární kombinace je rovna nulov vektoru. Při použití definice ?? můžeme říci, že vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jso neárně nezávislé, pokud z předpokladu $\alpha_1 \cdot \boldsymbol{x}_1 + \alpha_2 \cdot \boldsymbol{x}_2 + \cdots + \alpha_n \cdot \boldsymbol{x}_n$ nutně plyne, že $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

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

Pojem lineární závislosti a nezávislosti vektorů má v lineární algebře sadní důležitost. Závislost vektorů je možná názornější z pohledu následu věty ??, ovšem při ověřování lineární závislosti abstraktních vektorů je č definice ?? použitelnější. Má proto smysl definicím ?? a ?? věnovat nálež pozornost.

Uvažujme lineární prostor $\mathbf{R}^3$ (viz příklad ??, $n = 3$). Jsou dány tři vek 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. P poznámek ?? a ?? stačí zjistit, jaké mohou být koeficienty α, β, γ, pokud p žíme

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

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 $(0, 0, 0)$. I podle definice sčítání a násobení skalárem na $\mathbf{R}^3$ dostáváme

Tato soustava má nekonečně mnoho řešení (zkuste si to ověřit třeba Gausso eliminační metodou). Mezi těmito řešeními je jediné triviální, všechna ost jsou netriviální. Příkladem takového netriviálního řešení může být třeba α $\beta = -3$, $\gamma = -1$, 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 lovému vektoru, což podle definice ?? znamená, že vektory $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ jsou line závislé.

[lntrojka] 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. P poznámek ?? a ?? stačí zjistit, jaké mohou být koeficienty α, β, γ, pokud p žíme $\alpha\,\boldsymbol{x} + \beta\,\boldsymbol{y} + \gamma\,\boldsymbol{z} = \boldsymbol{o}$. 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 slo Musí tedy platit tyto rovnice:

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

Tato soustava má jediné řešení $\alpha = 0$, $\beta = 0$, $\gamma = 0$ (zkuste si to ověřit t

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

$$\alpha \cdot \sin(x) + \beta \cdot \cos(x) + \gamma \cdot 4 = 0 \quad \forall x \in \mathbf{R}(sincos4)$$

a zjistíme, jakých hodnot mohou nabývat koeficienty α, β, γ. Tato rovnost být splněna pro všechna $x \in \mathbf{R}$. Je možné, že při volbě tří hodnot x už vynutíme trivialitu lineární kombinace v (??). Zkusme štěstí například $x \in \left\{0, \frac{\pi}{2}, \pi\right\}$. V rovnici (??) se tedy omezíme na

$$\alpha \cdot \sin(x) + \beta \cdot \cos(x) + \gamma \cdot 4 = 0 \quad \text{pro } x \in \left\{0, \frac{\pi}{2}, \pi\right\}.(sincos4a)$$

Po dosazení hodnot x dostáváme tři rovnice:

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

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

[sincos42] Uvažujme lineární prostor všech reálných funkcí definovan 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 je lineární kombinaci rovnu nulové funkci:

$$\alpha \cdot \sin^2(x) + \beta \cdot 3\cos^2(x) + \gamma \cdot 4 = 0 \quad \forall x \in \mathbf{R}(sincos42)$$

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

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

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

Při vyšetřování lineární nezávislosti funkcí můžeme též využít deriv
Třeba rovnost (??) má platit pro všechna $x \in \mathbf{R}$ a tím pádem pro všechny
vace v libovolném bodě. Třeba v nule. Pro $x = 0$ je $\beta + 4\gamma = 0$, po zderivo
máme $\alpha\cos(x) - \beta\sin(x) = 0$ a dosazením $x = 0$ dostaneme druhou rov
$\alpha = 0$. Ještě jednou zderivjeme a dosadíme $x = 0$, máme $\beta = 0$. Z první
nosti plyne, že tedy musí $\alpha = 0$. Všechny koeficienty musejí být nulové, t
vektory f, g, h z příkladu ?? jsou lineárně nezávislé.

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

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

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

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 tato lineární kombinace jedině triviální, tj. všechny koeficienty jsou nulov

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

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

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

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

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

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

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
vektor $\boldsymbol{x}_r$ je roven lineární kombinaci ostatních vektorů. Dokážeme line
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 koefic
je jistě nenulový), která je rovna nulovému vektoru.

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

[lnlz] Nechť $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou prvky nějakého lineárního prostoru L.
platí:

(1) Lineární závislost či nezávislost vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ se nezmění při zn

(5) Jestliže jsou vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ lineárně nezávislé, pak jsou i vek
$\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{n-1}$ lineárně nezávislé.
(6) Samotný vektor $\boldsymbol{x}_1$ (chápaný ovšem jako skupina vektorů o jednom pr
je lineárně nezávislý právě tehdy, když je nenulový.
(7) Dva vektory jsou lineárně závislé právě tehdy, když jeden je násob
druhého.

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

(2) Vzhledem k vlastnosti (1) stačí bez újmy na obecnosti předpoklá
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 předpoklá
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 $\alpha_1 \boldsymbol{x}$
$\alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_n \boldsymbol{x}_n$ 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 n
vému vektoru.

(5) Dokážeme to sporem. Budeme předpokládat negaci tvrzení věty

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

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

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

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

[lzRn] Nechť $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m$ jsou vektory z lineárního prostoru $\mathbf{R}^n$. U žeme, že pokud $m > n$, jsou nutně tyto vektory lineárně závislé.

Podle definice lineární závislosti hledejme netriviální lineární kombin 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 neznám Protože pravé strany rovnic jsou nulové, soustava má určitě aspoň triviáln šení. Protože je v soustavě více neznámých než rovnic existuje nekonečně mn řešení této soustavy. Mezi těmito řešeními je jen jediné triviální a všec ostatní jsou netriviální.

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

[UOlnlz] Uvažujme lineární prostor U_O všech orientovaných úseček z

Abychom to dokázali, potřebujeme určitou představivost a zkušenosti s
klidovskou geometrií. Připomeňme, že O značí společný počátek všech orie
vaných úseček našeho lineárního prostoru. Zvolme nyní libovolnou orientova
úsečku $\boldsymbol{x}$ s počátkem v O, která leží v rovině určené úsečkami $\boldsymbol{u}, \boldsymbol{v}$. Ukážeme
existují $\alpha, \beta \in \mathbf{R}$ tak, že $\boldsymbol{x} = \alpha\,\boldsymbol{u} + \beta\,\boldsymbol{v}$. Leží-li $\boldsymbol{x}$ na společné přímce s úseč
$\boldsymbol{u}$ nebo na přímce společné s úsečkou $\boldsymbol{v}$, pak je $\boldsymbol{x}$ násobkem této úsečky a dr
koeficient hledané lineární kombinace je nulový. Nechť tedy $\boldsymbol{x}$ neleží na žá
z těchto přímek. Nakreslíme na tyto přímky měřítka, jako v příkladu ??. K
cový bod úsečky $\boldsymbol{x}$ označme X. Veďme bodem X rovnoběžky s oběma měř
Hodnota na měřítku podél vektoru $\boldsymbol{u}$ v místě průsečíku rovnoběžky s m
kem je číslo α. Číslo β je pak v místě průsečíku druhé rovnoběžky na dru
měřítku. Z definice sčítání orientovaných úseček pomocí rovnoběžníka vid
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 linea
závislé, protože z (2) plyne, že jedna z nich je lineární kombinací ostatn
Dále použijeme větu ??.

(4) Pokud $\boldsymbol{u}$ a $\boldsymbol{v} \in U_O$ jsou lineárně nezávislé a $\boldsymbol{w}$ leží mimo rovinu da
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 lin
ních kombinací

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

vyplňuje celý lineární prostor U_O.

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

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

* [neklz] Nechť L je lineární prostor a nechť $M \subseteq L$ je neprázdná mno vektorů. Množina M je *lineárně závislá*, pokud existuje konečně mnoho různ vektorů z M, které jsou lineárně závislé. Množina M je *lineárně nezáv* pokud není lineárně závislá. Tedy pokud neexistuje žádná její konečná line závislá podmnožina.

Prázdnou množinu považujeme vždy za lineárně nezávislou.

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

[lnnekmnozin] Uvědomíme si podrobněji základní vlastnost lineárně n vislých množin.

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

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

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

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

tři orientované úsečky lineárního prostoru U_O (viz příklad ??) ležící ve
lečné rovině, ale žádné dva neleží na společné přímce. Množinu těchto tří
torů označme M. Pak každá podmnožina N množiny M, $N \neq M$, je line
nezávislá, ale M je lineárně závislá.

[lnpolynomy] Nechť $M = \{1, x, x^2, x^3, \ldots\}$ je nekonečná podmnožina
árního prostoru všech polynomů P. Ukážeme, že M je lineárně nezávislá.

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

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

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

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

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

* [linobal] Nechť L je lineární prostor. *Lineární obal* skupiny vek
$\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ značíme $\langle \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \rangle$ a je to množina všech lineárních k
binací vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$.

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

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

[poznkonlob] Podle definice ?? je

V lineární algebře se nikdy nepracuje s nekonečným součtem násobků tor̊u, všechny lineární kombinace musejí být vždy tvořeny konečným souč Definice ?? připouští, že množina vektorů M může být nekonečná, ale i v t vém případě lineární obal sestavujeme z *konečných* součtů, tj. vybíráme kon podmnožiny vektorů z M, ze kterých sestavujeme lineární kombinace. Sa zřejmě, že takových výběrů může být nekonečně mnoho a z každého konečn výběru vektorů můžeme sestavit nekonečně mnoho lineárních kombinací. Ta lineární obal je nekonečná množina (s jedinou výjimkou: lineární obal nulov vektoru nebo prázdné množiny).

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

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

[obaltrojky] Jsou dány $\boldsymbol{x} = (1,2,3)$, $\boldsymbol{y} = (1,0,2)$, $\boldsymbol{z} = (-2,1,0)$. Ukáže že $\langle \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \rangle = \mathbf{R}^3$.

Množina lineárních kombinací prvků nějakého lineárního prostoru vždy podmnožinou L. Jde tedy pouze o to ukázat, že $\mathbf{R}^3 \subseteq \langle \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \rangle$. Vo 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 tom potřeba najít lineární kombinaci vektorů $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$, která je rovna vektoru $(a,$ 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

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

Například Gaussovou eliminační metodou zjistíme, že soustava má řešení

* [loblob] Nechť L je lineární prostor a $M \subseteq L$. Pak platí:

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

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

(2) Nechť $\boldsymbol{z} \in \langle N \rangle$, tj. předpokládáme, že $\boldsymbol{z}$ lze zapsat jako lineární k
binaci konečně mnoha prvků z N. Protože tyto prvky leží i v M, můžeme
že $\boldsymbol{z}$ lze zapsat jako lineární kombinaci konečně mnoha prvků z M. To p
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 $\langle\langle M$
$\langle M \rangle$. Nechť $\boldsymbol{z} \in \langle \langle M \rangle \rangle$, ukážeme že $\boldsymbol{z} \in \langle M \rangle$. Protože $\boldsymbol{z} \in \langle \langle M \rangle \rangle$, exis
vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \in \langle M \rangle$ takové, že platí (??). Pro každé $i \in \{1, \ldots, n$
$\boldsymbol{x}_i \in \langle M \rangle$, tj. existuje konečně mnoho vektorů $\boldsymbol{y}_{i,1}, \ldots, \boldsymbol{y}_{i,k_i} \in M$ takových

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

Dosazením těchto rovnic do (??) a roznásobením dostáváme výsledek, ž
je lineární kombinací konečně mnoha vektorů $\boldsymbol{y}_{i,j} \in M$, $i \in \{1, \ldots, n\}$,
$\{1, \ldots, k_i\}$. 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 $\boldsymbol{z} \in \langle$
je $M \cup \{\boldsymbol{z}\} \subseteq \langle M \rangle$ a podle (2) a (3) dostáváme $\langle M \cup \{\boldsymbol{z}\} \rangle \subseteq \langle \langle M \rangle \rangle = \langle$
Máme tedy $\langle M \rangle \subseteq \langle M \cup \{\boldsymbol{z}\} \rangle \subseteq \langle M \rangle$, takže v místě inkluzí musí být rovn

Vlastnost (1) věty ?? lidově řečeno znamená, že „lineární obalení“

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

Zbývá dokázat „je-li $\langle M\rangle = M$, pak M je lineární podprostor“. Uvažu
$\boldsymbol{x} \in M$, $\boldsymbol{y} \in M$. Abychom dokázali, že M je lineární podprostor, stačí ov
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
Protože $\boldsymbol{x} \in M$, $\boldsymbol{y} \in M$, je podle definice lineárního obalu každá jejich line
kombinace prvkem $\langle M\rangle$ a podle předpokladu je $\langle M\rangle = M$. V množině M
leží i uvedené dvě lineární kombinace vektorů $\boldsymbol{x}, \boldsymbol{y}$.

* [lobjemin] Nechť L je lineární prostor a $M \subseteq L$ je libovolná nepráz
množina. Pak $P = \langle M\rangle$ je nejmenší lineární podprostor, pro který platí M

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

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

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

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

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

[lnMcupN] Nechť M a N jsou lineárně nezávislé množiny v lineárním
storu L a předpokládejme, že $\langle M \rangle \cap \langle N \rangle = \{\boldsymbol{o}\}$. Pak množina $M \cup N$ je line
nezávislá.

Důkaz. Lineární nezávislost množiny $M \cup N$ vyplyne z toho, že každá kone
lineární kombinace vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m$ z M a vektorů $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_n$
(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 $\boldsymbol{b} \in \langle N \rangle$.
tože je $\boldsymbol{a} = -\boldsymbol{b}$ (jinak by součet nemohl být roven nulovému vektoru
také $\boldsymbol{a} \in \langle N \rangle$. Takže $\boldsymbol{a} \in \langle M \rangle \cap \langle N \rangle$ a podle předpokladu je $\boldsymbol{a} = \boldsymbol{o}$.
tože je M lineárně nezávislá, musí být lineární kombinace v první záv
pouze triviální. Je totiž rovna nulovému vektoru $\boldsymbol{a}$. Protože je N lienárně
závislá, musí být lineární kombinace v druhé závorce pouze triviální. Je t
rovna nulovému vektoru $-\boldsymbol{a}$. Takže zkoumaná lineární kombinace všech vek
$\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_n$ je triviální.

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

[N=N1cupN2] Nechť N je lineárně nezávislá množina v linerním pros
L a nechť N_1 a N_2 jsou její disjunktní podmnožiny (tj. $N_1 \cap N_2 = \emptyset$).
$\langle N_1 \rangle \cap \langle N_2 \rangle = \{\boldsymbol{o}\}$.

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

[lnlob] Nechť L je lineární prostor. Množina $N \subseteq L$ je lineárně nezáv
právě tehdy, když pro všechny vlastní podmnožiny $M \subset N$, $M \neq N$ p
$\langle M \rangle \subset \langle N \rangle$, $\langle M \rangle \neq \langle N \rangle$.

Důkaz (pro hloubavé čtenáře). Předpokládejme nejprve, že N je lineárně
závislá. Nechť $M \subset N$, $M \neq N$. Zvolme vektor $\boldsymbol{z} \in N$ takový, že $\boldsymbol{z} \notin$
Vektor $\boldsymbol{z}$ nelze vyjádřit jako lineární kombinaci žádné konečné podmno
prvků množiny M. Kdyby to bylo možné, byla by množina N lineárně záv
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 os
ních vektorů z N, takže $\boldsymbol{z} \in \langle M \rangle$, kde $M = N \setminus \{\boldsymbol{z}\}$. Podle vlastnosti (4) vět
je $\langle M \rangle = \langle M \cup \{\boldsymbol{z}\} \rangle$, jinými slovy $\langle M \rangle = \langle N \rangle$.

V této kapitole jsme definovali lineární závislost a nezávislost vektorů
??, ??, ??/. Vektory jsou lineárně závislé, pokud exituje netriviální line
kombinace těchto vektorů rovnající se nulovému vektoru. To je ekvivale
s tím, že existuje jeden vektor, který je lineární kombinací ostatních /
Vektory jsou lineárně nezávislé, pokud jen jejich triviální lineární kombinac
rovna nulovému vektoru. Tedy pokud neexistuje žádný takový vektor, ktery
byl lineární kombinací ostatních.

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

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

3. Báze, dimenze, souřadnice

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

* [dbase] *Báze* lineárního (pod)prostoru L je taková podmnožina $B \subseteq$
pro kterou platí

$$
\begin{aligned}
&(1) \quad B \text{ je lineárně nezávislá,}\\
&(2) \quad \langle B \rangle = L.
\end{aligned}
$$

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

[baseR3] Množina vektorů $B = \{(1,2,3),(1,0,2),(-2,1,0)\}$ je bází
árního prostoru $\mathbf{R}^3$, protože je podle příkladu ?? lineárně nezávislá a p
příkladu ?? generuje $\mathbf{R}^3$.

[gbaseR3] Množina vektorů $B = \{(1,0,0),(0,1,0),(0,0,1)\}$ je bází lin
ního prostoru $\mathbf{R}^3$. Snadno zjistíme, že je lineárně nezávislá a navíc pro ve
$(a,b,c) \in \mathbf{R}^3$ 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
neboli $\langle B \rangle = \mathbf{R}^3$.

Všimněme si, že jsme už našli dvě báze lineárního prostoru $\mathbf{R}^3$ (v
kladu ?? a v tomto příkladu). Vidíme tedy, že báze není určena lineárním

[basepolynomy] Množina $B = \{1, x, x^2, x^3, \ldots\}$ tvoří bázi lineárního storu P všech polynomů. Podle příkladu ?? je lineárně nezávislá. Zbývá ověřit, že $\langle B \rangle = P$. Zvolme nějaký polynom $p \in P$. Ukážeme, že $p \in \langle B \rangle$. každý polynom $p \in P$ existuje $n \in \mathbf{N}$ a reálná čísla $a_0, a_1, \ldots, a_n$ takov 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, je lineární kombinací prvků z K (koeficienty této lineární kombinace jsou $a_0, a_1, \ldots, a_n$). Z toho plyne, že $p \in \langle B \rangle$.

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

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

[dimUO] Vraťme se k lineárnímu prostoru U_O všech orientovaných úse se společným počátkem. Podle (5) z příkladu ?? je každá lineárně nezáv množina vektorů $\{\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}\}$ bází lineárního prostoru U_O.

* [jednoznacnostbase] *O existenci a jednoznačnosti báze.* Příklad ?? stroval skutečnost, že báze lineárního (pod)prostoru není určena jednozna Lineární (pod)prostor může mít dokonce nekonečně mnoho bází.

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

(2) Pro každou množinu M generátorů prostoru L existuje báze B prostor
taková, že $B \subseteq M$.

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

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

Princip maximality říká, že máme-li množinu $\mathcal{S}$ uspořádanou relací $\le$
platí-li, že každá podmnožina $\mathcal{R}$ množiny $\mathcal{S}$, ve které jsou si v relaci všec
prvky vzájemně, má horní mez $U \in \mathcal{S}$ (tj. $\forall R \in \mathcal{R}$ je $R \le_S U$), pak pro ka
prvek $N \in \mathcal{S}$ existuje maximální prvek $B \in \mathcal{S}$ tak, že $N \le_S B$. Maxim
prvek $B \in \mathcal{S}$ ja takový, že v $\mathcal{S}$ neexistuje prvek větší, tj. neexistuje p
$B' \in \mathcal{S}$, $B' \ne B$ tak, že $B \le_S B'$.

Pro důkaz první části věty nechť $\mathcal{S}$ je systém všech lineárně nezávis
množin lineárního prostoru L uspořádaný relací „být podmnožinou“, tj. re
$\subseteq$. Pro každý podsystém $\mathcal{R}$, kde lze relací $\subseteq$ porovnat každou množinu s kaž
(jedná se tedy o systém vzájemně do sebe vnořených množin R_I) sestro
$U = \cup R_I$. To je horní mez, protože $R_J \subseteq \cup R_I$ pro libovolnou množinu R
$\mathcal{R}$ a navíc $U \in \mathcal{S}$, neboť je lineárně nezávislá. Proč je nezávislá? Pro s

Množina B je báze, protože je lineárně nezávislá a přidáním libovolného pr
k B už získáme množinu mimo $\mathcal{S}$, tedy množinu lineárně závislou. Takže p
věty ?? musí $\langle B\rangle = L$.

K důkazu druhé čáti věty zvolíme $\mathcal{S}$ systém všech lineárně nezávislých p
množin množiny M uspořádaných relací $\subseteq$. Z principu maximality (podmí
se ověří stejně jako před chvílí) existuje ke množině $N = \emptyset$ maximální mno
$B \in \mathcal{S}$ taková, že $\emptyset \subseteq B$. Platí $M \subseteq \langle B\rangle$. Kdyby totiž $\boldsymbol{x} \in M$ a souča
$\boldsymbol{x} \notin \langle B\rangle$, pak $B \cup \{\boldsymbol{x}\}$ by byla podle věty ?? lineárně nezávislá podmno
M. To ale není možné, protože B je maximální. Na nerovnost $M \subseteq \langle B\rangle$
uplatníme větu ??: $\langle M\rangle \subseteq \langle\langle B\rangle\rangle = \langle B\rangle$. Protože $\langle M\rangle = L$, je $\langle B\rangle = L$..

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

Pokud už $\langle N\rangle = \mathbf{R}^n$, pak N samotná je báze a položíme $B = N$. Po
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, zd
$N \cup \{\boldsymbol{x}\}$ je báze. Podle věty ?? tato množina zůstává lineárně nezávislá. Po
$\langle N \cup \{\boldsymbol{x}\}\rangle = \mathbf{R}^n$, pak jsme našli bázi. Jestliže tato vlastnost neplatí, opaku
postup s přidáním dalšího prvku $\boldsymbol{y} \notin \langle N \cup \{\boldsymbol{x}\}\rangle$ znovu. Tento postup bud
opakovat tak dlouho, dokud budou existovat vektory mimo lineární obal
postupně rozšiřované množiny. Podle příkladu ?? dospějeme k výsledku po
nečně mnoha krocích, protože v $\mathbf{R}^n$ nelze vytvořit lineárně nezávislou množ
která by měla více než n prvků.

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

[M-base] Tvrzení druhé části věty ?? si ilustrujeme na příkladu kon prvků). Je možné, že takových množin s nejmenším počtem prvků bude exi vat více, pak je jedno, kterou z nich zvolíme. Označme ji B. Víme, že $\langle B\rangle$ (tuto vlastnost mají všechny podmnožiny A_i, takže jmenovitě též množina Dále víme, že odebráním jakéhokoli prvku z množiny B už nebude pro vou B_1 platit $\langle B_1\rangle = L$. Kdyby to platilo, tak nebyla vybrána B s nejmen počtem prvků. Nyní použijeme větu ??. Množina B je tedy lineárně nezáv

* [odebirani] Z konečné množiny M, která splňuje $\langle M\rangle = L$, lze vytv postupným odebíráním prvků z M bázi L, tedy najít množinu B z předcho příkladu. Existuje k tomu tento názorný postup: Je-li M lineárně nezáv je $B = M$ a jsme hotovi. Je-li lineárně závislá, podle věty ?? existuje je prvek M, který je lineární kombinací ostatních. Odebráním tohoto prvku vzn 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 opakuje tj. odebereme z M' vektor tak, že se nezmění lineární obal a znovu se pt na lineární nezávislost zbylé množiny. Proces končí, až se podaří odebrat t prvků, že zbytek je množina lineárně nezávislá. Proces určitě skončí po kon mnoha krocích, neboť M je konečná. Pokud M obsahuje nenulové vekt výsledná množina B je jistě neprázdná, lineárně nezávislá a $\langle B\rangle = L$, ted je báze.

Příklad báze prostoru F_D všech funkcí definovaných na množině D nebudeme uvádět, protože nemáme prostředky, jak takovou bázi zapsat. je v tomto případě nekonečnou množinou, která má větší mohutnost, ne mohutnost množiny přirozených čísel. Není tedy možné bázové prvky očísl a seřadit za sebe.

Ukážeme, že dvě (obecně různé) báze stejného lineárního (pod)pros mají stejný počet prvků. Tento důkaz se tradičně opírá o Steinitzovu o výměně. Čtenář si může pro větší názornost vytvořit množinu M čern kamínků a lineárně nezávislou množinu N bílých kamínků, které všechny le lineárním obalu černých. Může začít *vyměňovat* postupně černé kamínky za platí:

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

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

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

Nechť nyní věta platí pro každou lineárně nezávislou množinu s k prvk
dokážeme, že platí i pro množinu s $k+1$ prvky. Nechť $N = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k, \boldsymbol{v}_k$
$\langle M \rangle$. Označme $N_1 = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k\}$. Z množiny M lze odebrat k vektorů
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 $\boldsymbol{v}_{k}$
$\langle M \rangle = \langle M_1 \cup N_1 \rangle$ a ze čtvrté vlastnosti věty ??. Stačí tedy najít v M_1
tor $\boldsymbol{w}_1$ tak, aby jej šlo odebrat a obal se nezměnil, tedy $\langle M_1 \cup N \rangle = \langle$
$\{\boldsymbol{w}_1\} \cup N \rangle$. Protože $\boldsymbol{v}_{k+1} \in \langle M \rangle = \langle M_1 \cup N_1 \rangle$, existuje konečně mnoho vek
$\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_n \in M_1$ 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 $\boldsymbol{v}_{k+1}$ nenu
a (B) při $k > 0$ nesmí $\boldsymbol{v}_{k+1}$ být lineární kombinací vektorů $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots$
(věta ??). Z toho plyne, že $n > 0$ a nemohou být všechny koeficienty α_i nul
Uspořádáme nyní $\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_n$ tak, aby $\alpha_1 \neq 0$. Z předchozí rovnosti pl

[steinitz2] Nechť L je lineární prostor, $M \subseteq L$ je libovolná konečná mno a $N \subseteq \langle M \rangle$ je lineárně nezávislá množina. Pak počet prvků množiny N je m nebo roven počtu prvků množiny M.

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

* [stejnebase] Dvě báze stejného lineárního prostoru jsou obě nekon nebo mají stejný počet prvků.

Důkaz. Uvažujme dvě konečné báze B_1 a B_2 lineárního prostoru L. Pro $B_1 \subseteq \langle B_2 \rangle$ a B_1 je lineárně nezávislá, musí podle věty ?? mít B_2 aspoň t prvků, jako má B_1. Protože $B_2 \subseteq \langle B_1 \rangle$ a B_2 je lineárně nezávislá, musí p stejné věty mít B_1 aspoň tolik prvků, jako má B_2. Takže počet prvků tě množin musí být stejný.

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

* [ddimense] *Dimenze* lineárního (pod)prostoru L je počet prvků báze hoto (pod)prostoru L. Dimenzi (pod)prostoru L označujeme symbolem di Dimenzi jednobodového lineárního (pod)prostoru $L = \{\boldsymbol{o}\}$ pokládáme ro nule.

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

dim $\mathbf{R}^n = n$, viz příklad ??. dim $P_{\leq n} = n + 1$, viz příklad ??. dim $P =$
viz příklad ??. Konečně dim $U_{\mathbb{C}} = 3$ podle příkladu ??. Važme si toho

P je lineárně nezávislá množina, pro kterou je $B_P \subseteq \langle B_L \rangle$. Podle věty ?? B_P nejvýše tolik prvků, jako B_L.

[P=L] Nechť L je lineární prostor a $P \subseteq L$ je lineární podprostor lineár prostoru L. Nechť dále $\dim P = \dim L$ a tato dimenze je konečná. Po $P = L$.

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

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

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

[rovnostobalu] Nechť $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k, \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$ jsou vektory lineár 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 e valentní podmínce:

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

Důkaz. Přepokládejme nejprve rovnost obalů a dokážeme podmínku. O číme $U = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k\}$ a $V = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m\}$. Jestliže $\langle U \rangle = \langle V \rangle$, $U \subseteq \langle U \rangle = \langle V \rangle$, $V \subseteq \langle U \rangle = \langle V \rangle$, tedy $U \cup V \subseteq \langle U \rangle = \langle V \rangle$. Přechodem k lin [pribaleni] Nechť $\boldsymbol{v}, \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ jsou vektory lineárního prostoru L. $\boldsymbol{v} \in \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle$ právě tehdy, když $\dim\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle = \dim\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots$

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 o $\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle$ a $\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k, \boldsymbol{v} \rangle$ se rovnají. Proto se rovnají i jejich menze.

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

[123] Nechť L je lineární prostor, $\dim L = n$ a $M = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m\}$. 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 nahradi prvků z B všemi prvky z M tak, že se lineární obal nezmění. Aby to bylo m 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 $\boldsymbol{x} \notin \langle$ a přitom podle věty ?? zůstane rozšířená množina lineárně nezávislá. To podle (1) není možné. Musí tedy $\langle M \rangle = L$.

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

Množina $\{(1,1,1),(0,1,1),(0,0,2)\}$ je bází lineárního prostoru $\mathbf{R}^3$, pro 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

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

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

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

* [souradnice] Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je uspořádaná báze lineár prostoru L a $\boldsymbol{x} \in L$ je libovolný vektor. Uspořádanou n-tici reálných $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbf{R}^n$ nazýváme *souřadnicemi vektoru $\boldsymbol{x}$ vzhledem k usp dané 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 usp dané bázi (B) budeme zapisovat takto:

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

Jednoznačnost: Důkaz se opírá o lineární nezávislost množiny B. Ozna $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$. Nechť $\boldsymbol{x}$ má soužadnice $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ a současně souřadnice $(\beta_1, \beta_2, \ldots, \beta_n)$. V obou případech se jedná o souřadnice vzhle ke stejné bázi (B). Ukážeme, že pak je $\alpha_i = \beta_i, \forall i \in \{1, \ldots, n\}$. Podle definic 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 triviáln neární kombinace může být rovna nulovému vektoru. Všechny koeficienty dené lineární kombinace musejí tedy být rovny nule. Tím dostáváme $\alpha_i =$ $\forall i \in \{1, \ldots, n\}$.

[sourpolynomu] Nechť L je lineární prostor polynomů nejvýše třetího st Najdeme souřadnice polynomu $p \in L$, $p(x) = 2x^3 + x^2 - 3x$ vzhledem k u řádané 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 lineár prostoru L, tj. zda platí vlastnosti (1) a (2) z definice ??. Položili by násled lineární kombinaci rovnu nulovému polynomu:

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

a zkoumali by, za jakých okolností lze rovnost splnit. Polynom je nulový tehdy, když jsou nulové všechny jeho koeficienty, což vede na homogenní stavu čtyř rovnic o neznámých $\alpha, \beta, \gamma, \delta$. Tu by Tomášové vyřešili, zjistili že má pouze nulové řešení, a proto jsou dané polynomy z množiny B line nezávislé. Dále by Tomášové použili vlastnost (3) věty ?? a prohlásili, že k množina B je lineárně nezávislá a obsahuje stejný počet vektorů, jako je

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

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

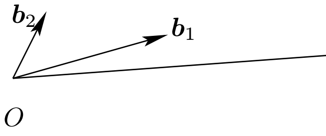
Soustava má jediné řešení $\alpha = 2, \beta = -1, \gamma = -5, \delta = 2$. Zapíšeme výsle
$\mathcal{C}_B(p) = (2, -1, -5, 2)$.

[sourpolynomu2] Uvažujme stejný lineární prostor L jako v předcho
příkladě a v něm stejný polynom $p \in L$, $p(x) = 2x^3 + x^2 - 3x$. Vzhle
k uspořádané bázi $B_0 = (1, x, x^2, x^3)$ má polynom souřadnice shodné se sv
koeficienty, tedy

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

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

[sourUO] 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 $\boldsymbol{x}$ vz
dem k uspořádané bázi $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2)$.

Je třeba narýsovat dvě měřítka, jedno procházející vektorem $\boldsymbol{b}_1$ a m
jedničku v koncovém bodě tohoto vektoru. Druhé měřítko prochází vekto
$\boldsymbol{b}_2$ a má jedničku v koncovém bodě $\boldsymbol{b}_2$. Obě měřítka mají nulu v bodě O.

U_O velmi obtížně uchopitelné. Je tedy užitečné přejít od těchto abstrakt vektorů k uspořádaným n-ticím reálných čísel, k jejich souřadnicím. S těm počítá daleko pohodlněji. Viz též příklad ??

[sourRn] V lineárním prostoru $\mathbf{R}^n$ se pracuje přímo s reálnámi čísly, ta hledat k uspořádaným n-ticím jejich souřadnice, tedy zase uspořádané n- může působit jako nošení dříví do lesa. Nicméně se o to pokusíme. Abych se do toho nezamotali, rozlišujme důsledně pojem *složky vektoru* od po *souřadnice vektoru* vzhledem ke zvolené bázi. Zvolíme dvě uspořádané bá $\mathbf{R}^3$:

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

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

Především je zřejmé, že B je báze (nevěřící Tomášové si to ověří). Mno 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), 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 ?? dostáv rovnost uspořádaných trojic $(1,2,3) = (\alpha+3\beta+2\gamma, 3\alpha+\gamma, \alpha+2\beta+\gamma$ této rovnosti plynou tři rovnice pro neznámé α,β,γ. Čtenář si sám spočíta soustava těchto tří rovnic má jediné řešení $\alpha = 9/4$, $\beta = 11/4$, $\gamma = -1$ 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 okam patrné, že $\mathcal{C}_{S_3}\big((1,2,3)\big) = (1,2,3)$. Poslední výsledek zobecníme v následuj tvrzení:

* Výše uvedené příklady ilustrují platnost sloganu „na volbě báze zále
Především vidíme, že souřadnice stejného vektoru vzhledem k různým bá
jsou rozdílné.

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

[dspoj] Nechť L je lineární prostor, M a N jsou jeho podprostory. Mno
$\langle M \cup N \rangle$ nazýváme *spojením podprostorů M a N* a značíme $M \vee N$.

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

[spojeni=soucet] Nechť L je lineární prostor, M a N jsou jeho podprost
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 p
z M a prvku z N, pak podle definice lineárního obalu je $\boldsymbol{x} \in \langle M \cup N \rangle = M$
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 exis
konečně mnoho prvků z M a konečně mnoho prvků z N takových, že
lineární kombinací těchto prvků. Tuto lineární kombinaci rozdělíme na so
násobků prvků z M a součet násobků ostatních prvků (tedy prvků z N). P
součet označíme $\boldsymbol{y}$ a druhý $\boldsymbol{z}$. Protože M a N jsou podprostory, je podle vět
$\langle M \rangle = M$, $\langle N \rangle = N$, takže lineární kombinace prvků z M leží v M a pod

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

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

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

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

Nyní ukážeme, že B je lineárně nezávislá množina. Položme

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

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

Lineárně nezávislou množinu vektorů, která generuje lineární (pod)pros
nazýváme bází tohoto (pod)prostoru /??/. Bází stejného (pod)prostoru je v
ale všechny mají stejný počet prvků /??, ??/. Tento počet prvků se naz
dimenze (pod)prostoru /??/.

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

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

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

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

4. Lineární zobrazení, izomorfismus

Zobrazení je zobecněním pojmu funkce. Zatímco funkce přiřazuje čís
čísla, zobrazení přiřazuje prvkům libovolné množiny prvky libovolné množ

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

[zobr] Nechť L_1 a L_2 jsou libovolné množiny. *Zobrazením $\mathcal{A}$ z množin*
do množiny L_2 rozumíme jakýkoli předpis, který každému prvku z množin
přiřadí jednoznačným způsobem nějaký prvek z množiny L_2. Skutečnost, ž
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
jaký prvek z množiny L_2. Tento prvek označujeme symbolem $\mathcal{A}(\boldsymbol{x})$ a nazýv
jej *hodnotou zobrazení $\mathcal{A}$ v $\boldsymbol{x}$* nebo také *obrazem prvku $\boldsymbol{x}$*. V tomto kontext
prvku $\boldsymbol{x}$ říká *vzor*. Je-li $M \subseteq L_1$, pak definujeme

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

[pZ] Pro ilustraci uvedeme příklady některých zobrazení:

(1) Funkce $f\colon \mathbf{R} \to \mathbf{R}$, která každému $x \in \mathbf{R}$ přiřadí $\sin(x) \in \mathbf{R}$ je spec
případ zobrazení.

(2) Zobrazení $\mathcal{A}_2$ z množiny diferencovatelných funkcí do množiny fun
které každé funkci přiřadí její derivaci. Tj. $\mathcal{A}_2(f) = f'$.

(3) Zobrazení $\mathcal{A}_3$ z množiny orientovaných úseček do množiny orientovan
úseček, které každému vektoru přiřadí jeho „stín“ na pevně zvolené ro
procházející počátkem.

(4) Zobrazení $\mathcal{A}_4$ z množiny spojitých funkcí do množiny reálných čísel, k
každé spojité funkci přiřadí hodnotu určitého integrálu této funkce od
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 posloupn
která každé funkci f přiřadí nekonečnou posloupnost $f(1), f(2), f(3)$

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

Zobrazení $\mathcal{A}$ z množiny L_1 na množinu L_2 je speciální případ zobraze množiny L_1 do množiny L_2 (všimneme si rozdílnosti slůvek „do“ a „na“). M se stát, že existují prvky $\boldsymbol{y} \in L_2$, pro které neexistuje žádný prvek $\boldsymbol{x} \in L_1$, k by splňoval $\mathcal{A}(\boldsymbol{x}) = \boldsymbol{y}$. V takovém případě zobrazení $\mathcal{A}$ není „na“ množinu je jenom „do“ množiny L_2. Lidově řečeno, množina L_2 je v takovém příp „větší“, než množina všech obrazů zobrazení $\mathcal{A}$.

[proste] Nechť L_1 a L_2 jsou libovolné množiny a uvažujme $\mathcal{A}\colon L_1 \to$ Zobrazení $\mathcal{A}$ je *prosté* (*injektivní*), pokud pro každé dva prvky $\boldsymbol{x}_1 \in L_1$, $\boldsymbol{x}$ 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“ množ říkáme mu *bijektivní* zobrazení.

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

* [linzob] Nechť L_1 a L_2 jsou lineární prostory, $\mathcal{A}\colon L_1 \to L_2$ je zobra z L_1 do L_2. Zobrazení $\mathcal{A}$ nazýváme *lineárním zobrazením*, pokud pro všec $\boldsymbol{x} \in L_1$, $\boldsymbol{y} \in L_1$, $\alpha \in \mathbf{R}$ platí

$$(1) \quad \mathcal{A}(\boldsymbol{x} + \boldsymbol{y}) = \mathcal{A}(\boldsymbol{x}) + \mathcal{A}(\boldsymbol{y}),$$

$$(2) \quad \mathcal{A}(\alpha \cdot \boldsymbol{x}) = \alpha \cdot \mathcal{A}(\boldsymbol{x}).$$

* Lineární zobrazení „zachovává“ operace sčítání a násobení konstan Sečteme-li dva prvky z L_1 a výsledek převedeme prostřednictvím lineár zobrazení do L_2, výjde totéž, jako kdybychom nejprve jednotlivé prvky vedli prostřednictvím zobrazení do L_2 a tam je sečetli. Všimneme si, že p

je nulový vektor lineárního prostoru L_1 a $\boldsymbol{o}_2$ je nulový vektor lineárního storu L_2.

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

Prozkoumáme linearitu zobrazení z příkladu ??.

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

Zobrazení $\mathcal{A}_4$ je lineární: $\int (f(x) + g(x))\mathrm{d}x = \int f(x)\mathrm{d}x + \int g(x)\mathrm{d}$ $\int (\alpha f(x))\mathrm{d}x = \alpha \int f(x)\mathrm{d}x$. 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 to případě sčítáme funkce, na prostoru L_2 sčítáme nekonečné posloupnosti. Zo zení $\mathcal{A}_6$ je lineární, protože $(c_1, c_2 \ldots) + (d_1, d_2 \ldots) = (c_1+d_1, c_2+d_2 \ldots)$ a o této posloupnosti je roven součtu obrazů jednotlivých posloupností $(c_1, c_2 \ldots$ $(d_1, d_2 \ldots)$. Na L_2 sčítáme funkce. Také platí $\alpha(c_1, c_2 \ldots) = (\alpha c_1, \alpha c_2, \ldots)$ a raz této posloupnosti je α-násobkem obrazu posloupnosti $(c_1, c_2 \ldots)$. Linea zobrazení $\mathcal{C}_B$, které každému vektoru přiřadí souřadnice, dokážeme v to textu později.

[R2toR3] Ověříme, zda je zobrazení $\mathcal{A}\colon \mathbf{R}^2 \to \mathbf{R}^3$, definované vzorcem

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

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

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

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

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

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

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

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

[principsupozice] Nechť L_1 a L_2 jsou lineární prostory. Zobrazení $\mathcal{A}\colon L$ L_2 je lineární právě tehdy, když pro všechna $\boldsymbol{x} \in L_1$, $\boldsymbol{y} \in L_1$, $\alpha \in \mathbf{R}$, β

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

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

Nad rovnítky jsme uvedli, kterou vlastnost jsme zrovna použili.

Opakovaným použitím principu superpozice (nebo formálně matematic indukcí) lze snadno dokázat, že $\mathcal{A}\colon L_1 \to L_2$ je lineární právě tehdy, když 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

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

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

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 mn
$\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_i \in M$ takových, že $\boldsymbol{x}$ je lineární kombinací těchto vektorů. Pro
$\mathcal{A}$ je lineární, máme podle (??)

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

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 existuje konečně mnoho $\boldsymbol{y}_i \in \mathcal{A}(M)$ takových, že $\boldsymbol{y}$ je lineární kombinací tě vektorů. Pro každý vektor $\boldsymbol{y}_i$ existuje vektor $\boldsymbol{x}_i \in M$ takový, že $\mathcal{A}(\boldsymbol{x}_i) =$
Máme tedy

* [jadro] Nechť L_1, L_2 jsou lineární prostory, $\boldsymbol{o}_2$ je nulový vektor v lin
ním 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 $\mathcal{A}$*.

[jadroprst] Jádro lineárního zobrazení $\mathcal{A}\colon L_1 \to L_2$ tvoří lineární pod
stor lineárního prostoru L_1

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

$$\mathcal{A}(\boldsymbol{x}) = \boldsymbol{o}_2, \quad \mathcal{A}(\boldsymbol{x}) = \boldsymbol{o}_2, \text{ takže } \mathcal{A}(\boldsymbol{x}+\boldsymbol{y}) = \mathcal{A}(\boldsymbol{x}) + \mathcal{A}(\boldsymbol{x}) = \boldsymbol{o}_2 + \boldsymbol{o}_2 = \boldsymbol{o}_2,$$
$$\text{dále } \mathcal{A}(\alpha\boldsymbol{x}) = \alpha\mathcal{A}(\boldsymbol{x}) = \alpha\boldsymbol{o}_2 = \boldsymbol{o}_2, \text{ takže také } \alpha$$

[kerR2toR3] Najdeme jádro zobrazení $\mathcal{A}$ z příkladu ??. Podle definic
je

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

Protože uspořádané trojice se rovnají, když se rovnají odpovídající složky, m
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 $\operatorname{Ker} \mathcal{A} = \big\{(0,0)\big\}$.

Uvedeme si jádra lineárních zobrazení z příkladu ??.

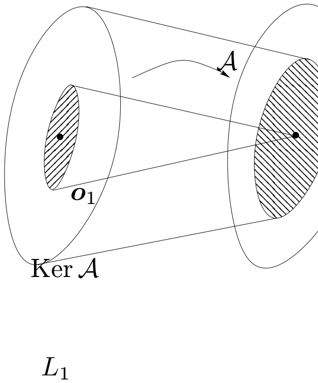
$\operatorname{Ker} \mathcal{A}_2$ je roven množině všech funkcí, které jsou konstantní. Právě
funkce se totiž zobrazí pomocí derivace na nulovou funkci.

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

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

* [defhod] *Defekt lineárního zobrazení* $\mathcal{A}\colon L_1 \to L_2$ 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

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



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 nerozlišite

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 $\mathcal{A}_2$ obsahuje jistě (kromě dalších funkcí) všechny polynomy, má tento prostor konečnou 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$\} = 1$. Pro $\mathcal{A}_3(U_O)$ obsahuje množinu všech vektorů, které leží v rovině, kam se prom stíny, je dimenze tohoto prostoru 2, neboli $\operatorname{hod} \mathcal{A}_3 = 2$. Zobrazení $\mathcal{A}_3$ se na klad používá v počítačové grafice, když je třeba 3D scénu zobrazit na stín monitoru. Rovnost def $\mathcal{A}$ ...

nespojité, ale L_1 obsahuje všechny funkce, tedy i nespojité funkce. $\operatorname{hod}\mathcal{A}_5 =$ protože množina $\mathcal{A}(L_1)$ obsahuje všechny nekonečné posloupnosti, jmeno tedy $(1,0,0,\ldots),(0,1,0,\ldots),\ldots$ a ty jsou lineárně nezávislé a je jich nekone mnoho.

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

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

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 kladu ?? má defekt roven nule. V příkladu ?? jsme totiž ukázali, že Ker $\{\boldsymbol{o}_1\}$. Spočítáme ještě $\operatorname{hod}\mathcal{A}$:

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

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

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

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

poznatku do původního vztahu máme $\boldsymbol{o}_1 = \alpha_1\,\boldsymbol{b}_1 + \alpha_2\,\boldsymbol{b}_2 + \cdots + \alpha_k\,\boldsymbol{b}_k$. Pro $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k\}$ je báze, musí $\alpha_i = 0$ pro všechny $i \in \{1, 2, \ldots, k\}$. Takže po triviální lineární kombinace množiny vektorů $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k, \boldsymbol{c}'_1, \boldsymbol{c}'_2, \ldots, \boldsymbol{c}'_m$ 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 tor $\boldsymbol{x}$ lze zapsat jako lineární kombinaci vektorů z $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k, \boldsymbol{c}'_1, \boldsymbol{c}'_2, \ldots,$ 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

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

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 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 mám 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 neko nou dimezi a je podprostorem lineárního prostoru L_1. Nechť konečně hod ∞. Pro spor předpokládejme, že $\dim L_1$ je konečná. Nechť $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$ báze L_1. Platí $\mathcal{A}(L_1) = \mathcal{A}(\langle \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k \rangle) = \langle \mathcal{A}(\boldsymbol{b}_1), \mathcal{A}(\boldsymbol{b}_2), \ldots \mathcal{A}(\boldsymbol{b}_k) \rangle$. P věty ?? tento obal nemůže obsahovat lineárně nezávislou množinu s vě počtem prvků než k, což je spor s tím, že $\operatorname{hod}\mathcal{A} = \infty$.

Povšimneme si, že věta $\operatorname{def}\mathcal{A} + \operatorname{hod}\mathcal{A} = \dim L_1$ „funguje“ ve všech pří dech lineárních zobrazení uvedených v příkladu ??. (2): $1 + \infty = \infty$, (3): $1 +$

že $\boldsymbol{x} - \boldsymbol{y} \in \operatorname{Ker} \mathcal{A}$, ale podle předpokladu víme, že $\boldsymbol{x} - \boldsymbol{y} \neq \boldsymbol{o}_1$ a souča
$\operatorname{Ker} \mathcal{A} = \{\boldsymbol{o}_1\}$. Spor.

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

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

Důkaz. Je-li M lineárně závislá, pak konečná pomnožina $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k\} \subseteq$
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 prin
superpozice dostáváme:

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

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

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

V předchozím textu jsme ukázali, že všechny ostatní „vlastnosti linear
(lineární podprostor, lineární obal, lineární závislost) se při lineárním zobra
nemění. V jakém případě se nemění lineární nezávislost ukazuje následující v

[zobN] Lineární zobrazení $\mathcal{A}$ zobrazuje lineárně nezávislé množiny v
na lineárně nezávislé množiny obrazů právě tehdy, když $\mathcal{A}$ je prosté zobraz

Obráceně, předpokládejme, že $\mathcal{A}$ je prosté a N je lineárně nezávislá n
žina. Pro spor budeme předpokládat, že $\mathcal{A}(N)$ je lineárně závislá. Pak n
existovat konečně mnoho $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k\} \subseteq N$, pro které lze najít nenulov
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

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

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 p
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
$\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k\}$ je podmnožinou N, takže tyto vektory jsou podle věty ??
árně nezávislé. Dále připomeňme, že ve vztahu $\alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \ldots + \alpha_n \boldsymbol{x}_n =$
existuje nenulové α_i. Dostáváme spor.

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

* [sour-lin] Nechť L je lineární prostor, $\dim L = n$ a nechť (B) je usp
daná báze prostoru L. Pak je zobrazení $\mathcal{C}_B : L \to \mathbf{R}^n$, které každému vek
$\boldsymbol{x} \in L$ přiřadí jeho souřadnice vzhledem k uspořádané bázi (B), zobraze
lineárním, prostým a na $\mathbf{R}^n$.

Důkaz. Věta ?? říká, že každému vektoru $\boldsymbol{x}$ lze jednoznačně přiřadit usp
danou n-tici souřadnic vzhledem k uspořádané bázi (B), takže $\mathcal{C}_B$ je zobra

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

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

Protože souřadnice vektoru vzhledem k bázi jsou určeny jednoznačně, z
dených rovností plyne, že $\mathcal{C}_B(\boldsymbol{x} \oplus \boldsymbol{y}) = \mathcal{C}_B(\boldsymbol{x}) + \mathcal{C}_B(\boldsymbol{y})$, $\mathcal{C}_B(\gamma\odot\boldsymbol{x}) = \gamma \cdot \mathcal{C}_B$
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 nenulov
vektoru se triviální lineární kombinace rovnat nemůže, je $\operatorname{Ker} \mathcal{C}_B = \{\boldsymbol{o}\}$, ne
$\operatorname{def} \mathcal{C}_B = 0$. 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 $\boldsymbol{x}$
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 $\mathcal{C}_B($
$\mathbf{R}^n$. Zobrazení $\mathcal{C}_B$ je tedy zobrazením z L „na“ $\mathbf{R}^n$. Je $\operatorname{hod} \mathcal{C}_B = \dim \mathbf{R}^n$

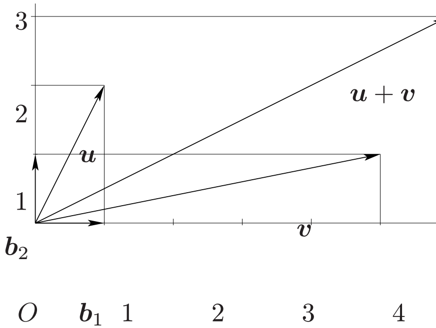
* [defiso] Lineární zobrazení $\mathcal{A}\colon L_1 \to L_2$, které je prosté a na L_2 se naz
izomorfismus. Existuje-li izomorfismus $\mathcal{A}\colon L_1 \to L_2$, říkáme, že prostory
L_2 *jsou izomorfní*, nebo že L_1 *je izomorfní* s L_2, resp. L_2 *je izomorfní* s L

Je zřejmé, že zobrazení $\mathcal{A}\colon L_1 \to L_2$, které je prosté a na L_2, ma
vlastnost, že každému $\boldsymbol{y} \in L_2$ lze jednoznačně najít $\boldsymbol{x} \in L_1$ tak, že $\mathcal{A}(\boldsymbol{x})$
Skutečně, pro daný obraz $\boldsymbol{y} \in L_2$ lze vzor $\boldsymbol{x} \in L_1$ najít, protože $\mathcal{A}$ je „na“
Přiřazení je jednoznačné, protože $\mathcal{A}$ je prosté. Toto „zpětné zobrazení“
do L_1 se nazývá *zobrazení inverzní* k zobrazení $\mathcal{A}$ a značíme je $\mathcal{A}^{-1}$. Pozd
této kapitole tento pojem zavedeme přesněji a ukážeme, že inverzní zobra
k lineárnímu zobrazení je rovněž zobrazení lineární. Takže inverzní zobraze
izomorfismu existuje a je rovněž izomorfizmus. To je důvod, proč v definic
izomorfních prostorů se nerozlišuje mezi tvrzeními „L_1 je izomorfní s L_2“ a
je izomorfní s L_1“.

* [isoRn] Každý lineární prostor L, pro který je $\dim L = n$, je izomo

prostoru $\mathbf{R}^n$. V tomto lineárním prostoru sčítáme a násobíme konstantou složkách, tedy pracujeme s reálnými čísly. Algoritmy, které řeší „otázky li rity“ v $\mathbf{R}^n$ jsou tedy založeny na numerických výpočtech. Složky vektorů z budeme v rámci těchto algorimů často zapisovat do řádků pod sebe, čímž v kají tabulky čísel, kterým říkáme *matice*. V následujících kapitolách zamě tedy pozornost na lineární prostor $\mathbf{R}^n$ a naučíme se pracovat s maticemi.

[U0isoR2] 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 pod-



prostoru P, musíme použít pravítko a kružítko, neboť sčítání je v to linárním prostoru definováno geometricky (viz příklad ??). Můžeme ale blém „sečtení těchto dvou vektorů“ přenést pomocí izomorfismu souřadni lineárního prostoru $\mathbf{R}^2$. Volbu báze a nalezení souřadnic vidíme na obrá Souřadnice vektoru $\boldsymbol{u}$ vzhledem k bázi $(\boldsymbol{b}_1, \boldsymbol{b}_2)$ jsou rovny $(1, 2)$ a souřad vektoru $\boldsymbol{v}$ vzhledem ke stejné bázi jsou $(5, 1)$. V lineárním prostoru $\mathbf{R}^2$ můž provést součet: $(1, 2) + (5, 1) = (6, 3)$. Tento výpočet jsme provedli *numer* Konečně je možné výsledek v $\mathbf{R}^2$ převést zpět do původního lineárního p prostoru P pomocí inverzního izomorfismu. V lineárním podprostoru P výsledek narýsujeme.

Nebo se můžeme ptát, zda vektory $\boldsymbol{u}$ a $\boldsymbol{v}$ jsou lineárně nezávislé v

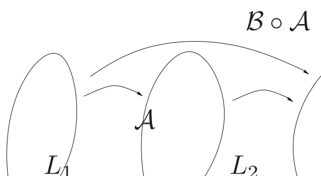
Ukážeme v následujících kapitolách, že lineární nezávislost řádků takové ma lze ověřit výpočtem determinantu matice **A** a ověřením, že je tento determi nenulový. V $\mathbf{R}^n$ tedy jsme schopni otázky linearity zkoumat numericky (pom algorimtů založených na počítání s čísly). Tento *numerický výpočet*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

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

V závěru této kapitoly zavedeme složené zobrazení, inverzní zobraze uvedeme jejich vlastnosti. K lineárním zobrazením se pak vrátíme ještě v k tole desáté, kde odhalíme mnoho dalších vlastností zejména v souvislosti s že mezi zobrazeními lineárních prostorů konečné dimenze a maticemi čís úzká souvislost.

[slozzob] Nechť $\mathcal{A}\colon L_1 \to L_2$ a $\mathcal{B}\colon L_2 \to L_3$ jsou zobrazení. Symbo $\mathcal{B} \circ \mathcal{A}\colon L_1 \to L_3$ označujeme *složené zobrazení*, které je definováno předpi $(\mathcal{B} \circ \mathcal{A})(\boldsymbol{x}) = \mathcal{B}\big(\mathcal{A}(\boldsymbol{x})\big)$, $\forall \boldsymbol{x} \in L_1$.

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"



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

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

[Izob] *Identické zobrazení* je zobrazení $\mathcal{I}\colon L \to L$, které je definov předpisem $\mathcal{I}(\boldsymbol{x}) = \boldsymbol{x}$. Stručně nazýváme zobrazení $\mathcal{I}$ *identitou*. Nechť $\mathcal{A}\colon L$ L_2 je prosté zobrazení. Pak definujeme *inverzní zobrazení* $\mathcal{A}^{-1}: \mathcal{A}(L_1)$ – jako takové zobrazení, které splňuje $\mathcal{A}^{-1} \circ \mathcal{A} = \mathcal{I}$, kde $\mathcal{I}\colon L_1 \to L_1$ je iden

[exIzob] Je-li $\mathcal{A}\colon L_1 \to L_2$ prosté, pak existuje právě jedno inverzní zo zení $\mathcal{A}^{-1}: \mathcal{A}(L_1) \to L_1$.

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

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

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

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 prvk $\boldsymbol{x} \in L_2$, $\boldsymbol{y} \in L_2$ musejí odpovídat různé prvky $\boldsymbol{a} \in L_1$ a $\boldsymbol{b} \in L_1$ takové $\mathcal{A}(\boldsymbol{a}) = \boldsymbol{x}$, $\mathcal{A}(\boldsymbol{b}) = \boldsymbol{y}$. Kdyby mělo platit $\boldsymbol{a} = \boldsymbol{b}$, okamžitě vidíme, že zobra $\mathcal{A}$ 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 $\mathcal{A}$ veden na nějaký prvek $\mathcal{A}(\boldsymbol{a}) = \boldsymbol{x} \in L_2$. Jinými slovy neexistuje prvek $\boldsymbol{a} \in$ který by neměl svůj protějšek $\mathcal{A}(\boldsymbol{a}) = \boldsymbol{x} \in L_2$.

* [sloziso] 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 $\mathcal{B}$ je izomorfismus.

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

* [isoLL] Každé dva lineární prostory stejné konečné dimenze jsou jemně izomorfní.

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

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

Zobrazení je lineární, pokud zobrazí součet vzorů na součet obrazů a

lineárního prostoru /??/. Dimenzi tohoto podprostoru říkáme defekt /??/. H
nost zobrazení je dimenze podprostoru všech obrazů. Součet defektu a hodn
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 zobra
na lineárně nezávislé množiny /??/. Lineární zobrazení které je prosté,
zachová všechny lineární vztahy mezi vzory i v postoru obrazů (závislost, n
vislost, báze, dimenze, podprostory, obaly). Je-li takové zobrazení navíc
prostor L_2, říkáme mu izomorfismus /??/.

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

5. Matice

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

[defmatice] *Matice typu (m, n)* je tabulka reálných (nebo komplexních
sel s m řádky a n sloupci. Číslo $a_{i,j}$ z i-tého řádku a j-tého sloupce této tab
nazýváme *(i, j)-tý prvek* matice. Množinu všech matic typu (m, n) zna
$\mathbf{R}^{m,n}$, 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 t
(m, n) nazýváme *čtvercovou maticí*, pokud $m = n$.

V následujícím textu budeme pracovat většinou s reálnými maticemi (
maticemi z $\mathbf{R}^{m,n}$). Skoro všechny vlastnosti lze analogicky odvodit i pro ma
komplexní. [rovnostmatic] Dvě matice *se rovnají*, pokud jsou stejného ty
všechny prvky jedné matice se rovnají odpovídajícím prvkům matice dr
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
$n = q$ a $a_{i,j} = b_{i,j}$ pro všechna $i \in \{1, 2, \dots, m\}$, $j \in \{1, 2, \dots, n\}$.

[deflpmatic] Nechť $\mathbf{A} = (a_{i,j}) \in \mathbf{R}^{m,n}$, $\mathbf{B} = (b_{i,j}) \in \mathbf{R}^{m,n}$. Matici
$\mathbf{R}^{m,n}$ nazýváme *součtem matic* $\mathbf{A}, \mathbf{B}$ (značíme $\mathbf{C} = \mathbf{A} + \mathbf{B}$), pokud pro p
matice $\mathbf{C} = (c_{i,j})$ platí $c_{i,j} = a_{i,j} + b_{i,j}$, $i \in \{1, 2, \dots, m\}$, $j \in \{1, 2,$

[maticeLP] Množina $\mathbf{R}^{m,n}$ tvoří se sčítáním matic a násobením ma reálným číslem podle definice ?? lineární prostor. Nulový vektor tohoto pros je nulová matice.

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

[matice32] 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 $\langle B$ $\mathbf{R}^{3,2}$. Nejprve ověříme lineární nezávislost. Položme lineární kombinaci pr z B rovnu nulové matici:

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

Odpovídající složky se musejí rovnat, což vede k šesti rovnicím: $\alpha = 0$, β $\gamma = 0$, $\delta = 0$, $\varepsilon = 0$, $\zeta = 0$. Jedině triviální lineární kombinace je ro 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 line

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

Důkaz. Věta je důsledkem věty ??.

[radkovevektory] Mezi lineárním prostorem $\mathbf{R}^n$ a lineárním prostorem I budeme používat následující izomorfismus: složky vektoru z $\mathbf{R}^n$ napíšem řadě (místo do řádku) do sloupce. Vzhledem k tomuto izomorfismu často tožňujeme vektory z $\mathbf{R}^{n,1}$ s vektory z $\mathbf{R}^n$ a mluvíme o *sloupcových vekto* Analogicky vektory z $\mathbf{R}^{1,n}$ nazýváme *řádkové vektory* a také je ztotožňuje vektory z $\mathbf{R}^n$.

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

[sim] Symbolem $\mathbf{A} \sim \mathbf{B}$ označujeme skutečnost, že matice $\mathbf{B}$ vzn z matice $\mathbf{A}$ konečným počtem kroků podle Gaussovy eliminační metody krok Gaussovy eliminační metody je považováno prohození řádků, pronásol řádku nenulovou konstantou, přičtení násobku řádku k jinému, odstranění lového řádku nebo přidání nulového řádku.

[symetriesim] Relace „$\sim$“ je symetrická, tj. $\mathbf{A} \sim \mathbf{B}$ právě tehdy, k $\mathbf{B} \sim \mathbf{A}$.

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

(1) Prohození dvou libovolných řádků mezi sebou. Stačí prohodit t

(4) Vynechání nebo přidání nulového řádku. Jestliže nulový řádek při chodu k matici **B** vynecháme, tak jej zas při návratu k matici **A** přidá Pokud jej při přechodu k matici **B** přidáme, pak jej při návratu k matic odebereme.

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

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

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

[lobradku] Množinu všech řádků matice **A** značíme r: **A**. Lineární množiny všech řádků matice **A** je tedy označen symbolem $\langle \mathrm{r}\colon \mathbf{A} \rangle$.

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

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

Všechny řádky matice $\mathbf{A}_1$ lze zapsat jako lineární kombinaci řádků ma **A**. Je přitom jedno, zda matice $\mathbf{A}_1$ vznikla prohozením řádků, pronásobe jednoho řádku nenulovým reálným číslem, přičtením násobku jednoho řá k jinému, odebráním nebo přidáním nulového řádku. Platí tedy, že r: **A** $\langle \mathrm{r}\colon \mathbf{A} \rangle$. 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 op lineárního prostoru $\mathbf{R}^5$.

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

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

* [dhodnost] *Hodnost matice* **A** značíme $\mathrm{hod}(\mathbf{A})$ a definujeme $\mathrm{hod}(\mathbf{A}$ $\dim\langle \mathrm{r}\colon \mathbf{A}\rangle$. * [hodAB] Je-li $\mathbf{A} \sim \mathbf{B}$, pak $\mathrm{hod}(\mathbf{A}) = \mathrm{hod}(\mathbf{B})$. Jinými slovy, G sova eliminační metoda nemění hodnost matice.

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

Matice $\mathbf{B}$ z příkladu ?? má zřejmě hodnost 3. Věta ?? nám zaručí, matice $\mathbf{A}$ z tohoto příkladu má hodnost 3.

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

[hod=maxradku] Hodnost matice je maximální počet lineárně nezávis řádků matice. Přesněji řečeno, hodnost je počet prvků největší lineárně n vislé podmnožiny z množiny řádků matice.

těch podmnožin, které jsou lineárně nezávislé. Řádky matice $\mathbf{A}'$ jsou totiž podprostoru $\langle \mathrm{r}\colon \mathbf{A}\rangle$ a kdyby existovala početnější lineárně nezávislá množin stejným lineárním obalem, byla by také bází téhož podprostoru. To ale možné, neboť dvě báze stejného lineárního (pod)prostoru mají podle věty stejný počet prvků. Počet řádků matice $\mathbf{A}'$ je podle definice ?? roven hodn matice $\mathbf{A}$.

Často je hodnost matice definována jako maximální počet lineárně n vislých řádků matice. Je ovšem potřeba si velmi pečlivě uvědomit, co s „maximální" v této formulaci znamená, a je potřeba z takové definice u dokázat větu ??.

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

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

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

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

[metodahodnosti] Předchozí věta nám společně s větou ?? dává záruky hodnost libovolné matice můžeme spočítat postupem, jaký jsme zvolili v kladu ??. Tedy při výpočtu hodnosti matice $\mathbf{A}$ ji převedeme Gaussovou el nační metodou na schodovitou matici $\mathbf{B}$ a v ní spočítáme počet nenulov řádků. Tento počet je roven hodnosti matice $\mathbf{B}$, protože její řádky jsou p věty ?? lineárně nezávislé a tvoří tedy bázi svého lineárního obalu. Kon $\operatorname{hod}\mathbf{A} = \operatorname{hod}\mathbf{B}$ díky větě ??.

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

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

(1) Počítáme modelové příklady a snažíme se držet malých celých č Přitom v prvním sloupci jsou nesoudělná čísla, což vede po eliminaci ke tečně velkým celým číslům. Poznamenejme ale, že modelové příklady ze sk se v praxi většinou nevyskytují, takže podstatnější pro nás bude druhý př využití.

(2) Při implementaci Gaussovy eliminačí metody do počítače je vh se snažit minimalizovat zaokrouhlovací chyby. Ty mohou nežádoucím zp

toto číslo nelze zjistit zcela přesně. Podívejme se kupříkladu na tuto matic

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

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

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

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

* [nezav=hod] Matice **A** má lineárně nezávislé řádky právě tehdy, k její hodnost je rovna počtu jejích řádků.

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

vává hodnost a je tedy v obou případech tato hodnost rovna počtu řádků n
menší než počet řádků. Podle věty ?? to znamená, že v obou případech
řádky linárně nezávislé nebo jsou v obou případech lineárně závislé.

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

Vektory $(1,2,3,4,5),(2,3,4,4,7),(1,1,1,3,4),(3,5,7,8,12)$ jsou line
závislé, protože odpovídající matice má hodnost 3, jak jsme již spočíta
příkladu ??.

[algolrovnost] Věta ?? společně s definicí hodnosti matice jako dim
lineárního obalu řádků matice ?? nám dává návod, jak vyhodnotit, zda
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 vek
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
tice $\mathbf{A}$ zapíšeme vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$, do řádků matice $\mathbf{B}$ zapíšeme vek
$\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$ a konečně do řádků matice $\mathbf{C}$ zapíšeme řádky obou matic
lečně. Pak uvedené lineární obaly se rovnají, pokud $\operatorname{hod}\mathbf{A} = \operatorname{hod}\mathbf{B} =$ ho
Přitom na výpočet hodnosti máme algoritmus ??.

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

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

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

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

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

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

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

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

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

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

[ATT=A] Pro každou matici $\mathbf{A}$ platí: $(\mathbf{A}^T)^T = \mathbf{A}$.

Důkaz. Věta plyne přímo z definice ??.

* [hA=hAT] 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 $\operatorname{hod}(\mathbf{A}^T) \geq \operatorname{hod}(\mathbf{A})$. N $\mathbf{A} \in \mathbf{R}^{m,n}$ a označme $k = \operatorname{hod}(\mathbf{A})$. Podle věty ?? existuje k lineárně nezávis řádků matice $\mathbf{A}$. Označme je $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$. Zapišme si, co to znamená, že řádky jsou lineárně nezávislé. Pro

$$\alpha_1 \boldsymbol{b}_1 + \alpha_2 \boldsymbol{b}_2 + \cdots + \alpha_k \boldsymbol{b}_k = \boldsymbol{o}$$

Koeficienty jednotlivých rovnic soustavy (??) odpovídají částem sloupců
tice $\mathbf{A}$. Částmi sloupců v tomto důkazu budeme označovat uspořádané k-
obsahující jen ty prvky z daného sloupce, které leží ve vybraných řád
$\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$. Aby bylo zaručeno pouze triviální řešení soustavy (??), mus
po přímém chodu Gaussovy eliminační metody dostat schodovitou matici
řádcích (méně řádků by vedlo na nekonečně mnoho řešení). To podle vě
a ?? znamená, že existuje k lineárně nezávislých částí sloupců matice $\mathbf{A}$. T
celé sloupce matice $\mathbf{A}$ jsou lineárně nezávislé (kdyby byly závislé, pak by st
netriviální lineární kombinace celých sloupců dávala nulový vektor i na čás
sloupců, ale my víme, že části sloupců jsou lineárně nezávislé). Máme tedy
ručeno, že v matici $\mathbf{A}$ je aspoň k lineárně nezávislých sloupců (zatím není
loučeno, že jich může být více). Podle věty ?? tedy je $\mathrm{hod}(\mathbf{A}^T) \geq k = \mathrm{hod}$

Máme $\mathrm{hod}\big((\mathbf{A}^T)^T\big) \geq \mathrm{hod}(\mathbf{A}^T) \geq \mathrm{hod}(\mathbf{A})$, a přitom podle věty ?
$(\mathbf{A}^T)^T = \mathbf{A}$, takže všechny uvedené hodnosti se rovnají.

Ukázali jsme, že hodnosti matice $\mathbf{A}$ a $\mathbf{A}^T$ se rovnají. To vysvětluje,
jsme nedefinovali zvlášť „řádkovou" hodnost matice jako dimenzi lineár
obalu řádků a zvlášť „sloupcovou" hodnost jako dimezi lineárního obalu slou
Tato čísla jsou podle věty ?? stejná.

[hodminimum] 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 m
nebo rovna počtu sloupců z věty ??.

Na konci kapitoly třetí jsme uvedli „přílepek" o spojení a průniku pod
storů. Nyní máme k dispozici větu ??, tedy aparát, pomocí kterého si můž
tuto problematiku ilustrovat na příkladech.

[pr-prunikspojeni] Jsou dány lineární podprostory M a N lineárního
storu $\mathbf{R}^5$ pomocí lineárních obalů:

matice, takže budeme eliminovat následující matice:

$$M: \quad \begin{pmatrix} 1 & 2 & 0 & 1 & 1 \\ 1 & 3 & 1 & 3 & 4 \\ 3 & 5 & 2 & 4 & 5 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 \\ 0 & -1 & 2 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 3 & 3 & 5 \end{pmatrix},$$

$$N: \quad \begin{pmatrix} 1 & 1 & 3 & 4 & 3 \\ 1 & 0 & 2 & 2 & 0 \\ 2 & 1 & 3 & 2 & 3 \\ 0 & 1 & 2 & 4 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 3 & 4 & 3 \\ 0 & -1 & -1 & -2 & -3 \\ 0 & -1 & -3 & -6 & -3 \\ 0 & 1 & 2 & 4 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 3 & 4 & 3 \\ 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 2 & 4 & 0 \\ 0 & 0 & 1 & 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

Podle věty ?? jsou řádky matic zapsaných nejvíce vpravo lineárně nezáv
Lineární obal těchto řádků zůstal zachován a je roven M, respektive N. M
tedy:

$$\text{báze } M: \quad \big\{(1,2,0,1,1),(0,1,1,2,3),(0,0,3,3,5)\big\}, \quad \dim M = 3,$$
$$\text{báze } N: \quad \big\{(1,1,3,4,3),(0,1,1,2,3),(0,0,1,2,0)\big\}, \quad \dim N = 3.$$

Vzhledem k tomu, že tři vektory, kterými je zadán podprostor M, jsou linea
nezávislé, můžeme zapsat i jinou bázi M: $\{(1,2,0,1,1),(1,3,1,3,4),(3,5,2,$
Vektory, kterými je zadán podprostor N jsou lineárně závislé, takže net
bázi.

Platí $M \vee N = \langle M \cup N \rangle = \langle \text{báze } M \cup \text{báze } N \rangle$, takže bázi tohoto p
prostoru najdeme eliminací následující matice:

$$M \vee N: \quad \begin{pmatrix} 1 & 2 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 3 & 3 & 5 \\ 1 & 1 & 3 & 4 & 3 \\ 0 & 1 & 1 & 2 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 3 & 3 & 5 \\ 0 & -1 & 3 & 3 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 3 & 3 & 5 \\ 0 & 0 & 4 & 5 & 5 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}$$

bohužel nalezení báze průniku dá ještě trochu práce. Vektory společné ob
podprostorům musí jít zapsat jako lineární kombinace báze M i lineární k
binace báze N:

$$\alpha\,(1,2,0,1,1)+\beta\,(0,1,1,2,3)+\gamma\,(0,0,3,3,5) = a\,(1,1,3,4,3)+b\,(0,1,1,2,3)$$

Z tohoto požadavku nám vychází soustava pěti rovnic o šesti neznámých α, β
Eliminujeme matici této homogenní soustavy.

$$\begin{pmatrix} 1 & 0 & 0 & -1 & 0 & 0 \\ 2 & 1 & 0 & -1 & -1 & 0 \\ 0 & 1 & 3 & -3 & -1 & -1 \\ 1 & 2 & 3 & -4 & -2 & -2 \\ 1 & 3 & 5 & -3 & -3 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 1 & -1 & 0 \\ 0 & 1 & 3 & -3 & -1 & -1 \\ 0 & 2 & 3 & -3 & -2 & -2 \\ 0 & 3 & 5 & -2 & -3 & 0 \end{pmatrix} \sim \cdots \sim \begin{pmatrix} 1 & 0 & 0 & - \\ 0 & 1 & 0 & \\ 0 & 0 & 3 & - \\ 0 & 0 & 0 & \end{pmatrix}$$

Volíme $b = t$, $c = u$, pak vychází $a = -u$. Ostatní hodnoty proměnn
nemusíme počítat a vrátíme se k pravé straně rovnosti (??). Vektory, které
společné oběma prostorům, musejí tedy splňovat:

$$-u\,(1,1,3,4,3)+t\,(0,1,1,2,3)+u\,(0,0,1,2,0) = t\,(0,1,1,2,3)+u\,(-1,-1,-$$

Je tedy $M \cap N = \big\langle (0,1,1,2,3), (1,1,2,2,3) \big\rangle$ a tyto dva vektory tvoří jed
možných bází lineárního prostoru $M \cap N$. Že průnik obsahuje vektor $(0,1,1,$
nás nepřekvapí, protože tento vektor byl součástí obou bází podprostorů
N. Soustavu jsme počítali jen kvůli tomu, abychom našli ten druhý vektor

Množina matic $\mathbf{R}^{m,n}$ tvoří lineární prostor. Vektory z $\mathbf{R}^n$ můžeme zto
nit s maticemi z $\mathbf{R}^{1,n}$ (řádkové vektory) nebo s maticemi z $\mathbf{R}^{n,1}$ (sloup
vektory). Řádkové vektory můžeme klást pod sebe a tvořit matice, nebo
žeme sloupcové vektory klást vedle sebe a rovněž dostáváme matice.

Hodnost matice je dimenze lineárního obalu řádků /??/, což je totéž
dimenze lineárního obalu sloupců /??/. Na výpočet hodnosti matice se pou

6. Násobení matic

* [soucinAB] Nechť $\mathbf{A} = (a_{i,j}) \in \mathbf{R}^{m,n}$ a $\mathbf{B} = (b_{j,k}) \in \mathbf{R}^{n,p}$. Pa
definován *součin matic* $\mathbf{A} \cdot \mathbf{B}$ (v tomto pořadí) jako matice typu (m, p) ta
každý prvek $c_{i,k}$ matice $\mathbf{A} \cdot \mathbf{B}$ je dán vzorcem

$$c_{i,k} = a_{i,1}\, b_{1,k} + a_{i,2}\, b_{2,k} + \cdots + a_{i,n}\, b_{n,k} = \sum_{j=1}^{n} a_{i,j}\, b_{j,k}, \quad i \in \{1, \ldots, m\}, \quad k \in$$

Všimneme si, že násobení je definováno jen tehdy, pokud počet slou
první matice je roven počtu řádků druhé matice. Výsledná matice má st
počet řádků, jako první matice a stejný počet sloupců, jako druhá ma
Názorně:

$$m\left\{ \underbrace{\begin{pmatrix} \circ & \circ & \cdots & \circ \\ \circ & \circ & \cdots & \circ \\ & & \cdots & \\ \circ & \circ & \cdots & \circ \end{pmatrix}}_{n} \right. \cdot \; n\left\{ \underbrace{\begin{pmatrix} \circ & \cdots & \circ \\ \circ & \cdots & \circ \\ \circ & \cdots & \circ \\ & \cdots & \\ \circ & \cdots & \circ \end{pmatrix}}_{p} \right. = \left. \underbrace{\begin{pmatrix} \circ & \cdots & \circ \\ \circ & \cdots & \circ \\ & \cdots & \\ \circ & \cdots & \circ \end{pmatrix}}_{p} \right\}$$

Každý prvek matice $\mathbf{A} \cdot \mathbf{B}$ přitom musíme počítat podle vzorce (??) jako
čet součinů odpovídajících prvků řádku první matice a sloupce druhé ma
Začátečníci mohou použít tzv. „dvouprstovou vizuální metodu“: při výp
čísla $c_{i,k}$ přiložte ukazováček levé ruky na začátek i-tého řádku první mati
ukazováček pravé ruky na začátek k-tého sloupce druhé matice. Pak pronás

[prikladnasobeni]

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 0 & 2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \\ 2 & 7 \end{pmatrix} = \begin{pmatrix} 1\cdot 1 + 2\cdot 3 + 3\cdot 5 + 4\cdot 2 & 1\cdot 2 + 2\cdot 4 + 3 \\ 5\cdot 1 + 6\cdot 3 + 7\cdot 5 + 8\cdot 2 & 5\cdot 2 + 6\cdot 4 + 7 \\ 0\cdot 1 + 2\cdot 3 + 1\cdot 5 + 0\cdot 2 & 0\cdot 2 + 2\cdot 4 + 1 \end{pmatrix}$$

* [nekomutuje]

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 \\ -2 & - \end{pmatrix}$$

Tento příklad ilustruje, že násobení matic obecně nesplňuje komutativní zá ani pro čtvercové matice, tj. existují matice **A**, **B**, pro které neplatí $\mathbf{A}\cdot\mathbf{B} = \mathbf{B}$ Pokud některá z matic **A**, **B** není čtvercová, pak součin $\mathbf{B}\cdot\mathbf{A}$ nemusí být vů definován, přestože součin $\mathbf{A}\cdot\mathbf{B}$ definován je.

Příklad dále ukazuje, že není splněna ani vlastnost nuly, na kterou j zvyklí při násobení reálných čísel: je-li $a \neq 0$, $b \neq 0$, pak $a\,b \neq 0$. V příkl násobíme dvě nenulové matice, a přitom dostáváme matici nulovou.

Musíme si z toho odnést ponaučení, že násobení matic nesplňuje všec vlastnosti, na které jsme zvyklí, a proto při úpravách vzorců obsahujících sobení matic si musíme dát pozor, co můžeme v dané situaci udělat.

Nabízí se přirozená otázka, zda násobení matic splňuje aspoň nějaké kony, na které jsme zvyklí (jinak by bylo skoro zbytečné tuto operaci nazy násobením). Následující věta ukazuje, že násobení matic je asociativní a distributivní vzhledem ke sčítání matic.

* [soucinAB-vlastnosti] Nechť $\alpha \in \mathbf{R}$ a matice **A**, **B**, **C** jsou odpovídají 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),

(1) Označme $\mathbf{A} = (a_{i,j})$, $\mathbf{B} = (b_{j,k})$, $\mathbf{C} = (c_{k,l})$, $\mathbf{A} \cdot \mathbf{B} = (d_{i,k})$, $\mathbf{B} \cdot$ $(f_{j,l})$, $(\mathbf{A} \cdot \mathbf{B}) \cdot \mathbf{C} = (g_{i,l})$, $\mathbf{A} \cdot (\mathbf{B} \cdot \mathbf{C}) = (h_{i,l})$ pro $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots$ $k \in \{1, \ldots, p\}$, $l \in \{1, \ldots, q\}$. Jde o to ukázat, že $g_{i,l} = h_{i,l}$ pro všec $i \in \{1, \ldots, m\}$ a $l \in \{1, \ldots, q\}$. Podle definice ?? je

$$d_{i,k} = \sum_{j=1}^{n} a_{i,j}\, b_{j,k}, \quad f_{j,l} = \sum_{k=1}^{p} b_{j,k}\, c_{k,l},$$

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 $a_{i,j} \cdot b_{j,k} \cdot$ můžeme zapsat do tabulky, ve které index j odpovídá řádku tabulky a in k sloupci. Hodnota X pak znamená součet sloupcových mezisoučtů v tab a hodnota Y součet řádkových mezisoučtů. Každá účetní ví, že obě hodn musí dát stejný výsledek. My ostatní to snadno nahlédneme.

(2) Označme $\mathbf{A} = (a_{i,j})$, $\mathbf{B} = (b_{i,j})$, $\mathbf{C} = (c_{j,k})$, $(\mathbf{A} + \mathbf{B}) \cdot \mathbf{C} = (d_{i,k})$ $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, n\}$, $k \in \{1, \ldots, p\}$. Pak podle definic ?? a ?? pla

$$d_{i,k} = \sum_{j=1}^{n} (a_{i,j} + b_{i,j})\, c_{j,k} = \sum_{j=1}^{n} (a_{i,j}\, c_{j,k} + b_{i,j}\, c_{j,k}) = \sum_{j=1}^{n} a_{i,j}\, c_{j,k} + \sum_{j=1}^{n} b_{i,j}$$

což odpovídá prvkům matice $\mathbf{A} \cdot \mathbf{C} + \mathbf{B} \cdot \mathbf{C}$.

což dokazuje vzorec: (4).

(5) Označíme $\mathbf{A} = (a_{i,j})$, $\mathbf{B} = (b_{j,k})$, $\mathbf{C} = \mathbf{A} \cdot \mathbf{B} = (c_{i,k})$, $i \in \{1, \ldots,$
$j \in \{1, \ldots, n\}$, $k \in \{1, \ldots, p\}$. Je tedy $\mathbf{A}^T = (\alpha_{j,i})$, $\mathbf{B}^T = (\beta_{k,j})$, kde $\alpha_{j,i} =$
$\beta_{k,j} = b_{j,k}$. Označme ještě součin $\mathbf{D} = \mathbf{B}^T \cdot \mathbf{A}^T = (d_{k,i})$. Podle definice náso
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).

Nechť $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ jsou čtvercové matice. Spočítáme $(\mathbf{A}+\mathbf{B})\cdot(\mathbf{B}+\mathbf{C})$. Podl
ve větě ?? je $(\mathbf{A} + \mathbf{B}) \cdot (\mathbf{B} + \mathbf{C}) = (\mathbf{A} + \mathbf{B}) \cdot \mathbf{B} + (\mathbf{A} + \mathbf{B}) \cdot \mathbf{C} = \mathbf{A} \cdot \mathbf{B} +$
$\mathbf{B} + \mathbf{A} \cdot \mathbf{C} + \mathbf{B} \cdot \mathbf{C}$. Místo zápisu $\mathbf{B} \cdot \mathbf{B}$ budeme užívat zkratku $\mathbf{B}^2$. Kon
výsledek je $\mathbf{A} \cdot \mathbf{B} + \mathbf{B}^2 + \mathbf{A} \cdot \mathbf{C} + \mathbf{B} \cdot \mathbf{C}$.

Jiný příklad: $(\mathbf{A} + \mathbf{B})^2 = (\mathbf{A} + \mathbf{B}) \cdot (\mathbf{A} + \mathbf{B}) = (\mathbf{A} + \mathbf{B}) \cdot \mathbf{A} + ($
$\mathbf{B}) \cdot \mathbf{B} = \mathbf{A}^2 + \mathbf{B}^2 + \mathbf{A} \cdot \mathbf{B} + \mathbf{B} \cdot \mathbf{A}$. Tento výsledek obecně nelze zjednodu
protože násobení matic není komutativní. Pouze tehdy, když pro tyto ma
platí $\mathbf{A} \cdot \mathbf{B} = \mathbf{B} \cdot \mathbf{A}$, můžeme psát výsledek ve tvaru $\mathbf{A}^2 + 2\,\mathbf{A} \cdot \mathbf{B} + \mathbf{B}^2$.

Matice může vzniknout sestavením menších matic vedle sebe anebo
sebe. Například:

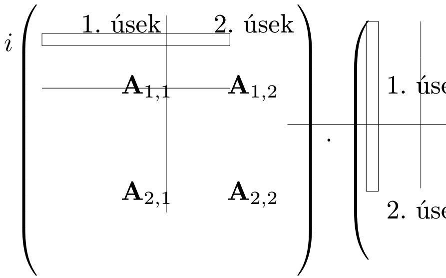
$$\mathbf{A}_1 = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad \mathbf{A}_2 = \begin{pmatrix} 6 \\ 7 \end{pmatrix}, \quad \mathbf{A}_3 = \begin{pmatrix} 8 & 9 \end{pmatrix}, \quad \mathbf{A}_4 = \begin{pmatrix} 0 \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} \mathbf{A}_1 \\ \mathbf{A}_3 \end{pmatrix}$$

Zde na matici $\mathbf{B}$ můžeme pohlížet jako na matici sestavenou například z b
$\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$, $\mathbf{A}_4$. Bloky kladené vedle sebe musejí mít samozřejmě stejný p
řádků a bloky kladené pod sebe musejí mít stejný počet sloupců.

[ctyribloky] Nechť $\mathbf{A}$ a $\mathbf{B}$ jsou matice sestavené po blocích takto:

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_{1,1} & \mathbf{A}_{1,2} \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} \mathbf{B}_{1,1} & \mathbf{B}_{1,2} \end{pmatrix}$$

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 ma-



tice $\mathbf{A}$ a druého úseku k-tého sloupce matice $\mathbf{B}$. Prvek $c_{i,k}$ je podle defi
maticového součinu ?? součtem odpovídajících prvků na i-tém řádku a k-
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 argument
v případě, že i-tý řádek nebo k-tý sloupec procházejí jinými bloky. Obtížn
o tom mluví, lepší je si toto maticové násobení „nakreslit“ (viz obrázek).

$$c'_{i,k} = \text{prvek}_{i,k} \text{ matice } \mathbf{A}_{1,1} \cdot \mathbf{B}_{1,1} = (1.\ \text{úsek } i\text{-tého řádku } \mathbf{A}) \cdot (1.\ \text{úsek } k\text{-t}$$

$$c''_{i,k} = \text{prvek}_{i,k} \text{ matice } \mathbf{A}_{1,2} \cdot \mathbf{B}_{2,1} = (2.\ \text{úsek } i\text{-tého řádku } \mathbf{A}) \cdot (2.\ \text{úsek } k\text{-t}$$

$$c_{i,k} = \text{prvek}_{i,k} \text{ matice } \mathbf{A} \cdot \mathbf{B} = (\text{celý } i\text{-tý řádek } \mathbf{A}) \cdot (\text{celý } k\text{-tý sloupec } \mathbf{B})$$

[soucinbloku] 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 $\mathbf{A}_{i,j} \cdot$

Důkaz. Je zřejmé, že $\mathbf{C}_{i,k}$ je blok typu (u_i, v_k), kde u_i je počet řádků bloku
a v_k je počet sloupců bloku $\mathbf{B}_{1,k}$ a tento typ mají všechny součiny $\mathbf{A}_{i,j} \cdot \mathbf{B}_{j,k}$
všechna $j \in \{1, \ldots, n\}$, takže součet součinů ve vzorci pro $\mathbf{C}_{i,k}$ je defino
Větu lze dále dokázat analogicky, jako větu předchozí. Každý řádek matic
a sloupec matice $\mathbf{B}$ se nyní rozdělí na n úseků.

Povšimneme si, že pokud volíme ve větě ?? za bloky „matice s jedi
číslem“ (matice z $\mathbf{R}^{1,1}$), pak věta rozepisuje definici maticového násobení.
jímavé jsou pro nás ještě případy, kdy matice $\mathbf{A}$ je rozepsána do řádkov
bloků nebo matice $\mathbf{B}$ je rozepsána do sloupcových bloků. To je formulován
následujících větě.

[soucinsloupcu] Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$, $\mathbf{B} \in \mathbf{R}^{n,p}$. Nechť matice $\mathbf{B}$ je zaps
po sloupcích: $\mathbf{B} = (\boldsymbol{b}_1 \ \boldsymbol{b}_2 \ \ldots \ \boldsymbol{b}_p)$, tj. $\boldsymbol{b}_k$ jsou sloupcové vektory z $\mathbf{R}^{n,1}$. Pa

$$\mathbf{A} \cdot \mathbf{B} = (\mathbf{A} \cdot \boldsymbol{b}_1 \quad \mathbf{A} \cdot \boldsymbol{b}_2 \quad \ldots \quad \mathbf{A} \cdot \boldsymbol{b}_p)$$

Důkaz. Stačí v předchozí větě ?? volit matici $\mathbf{A}$ obsahující jediný blok a ma
$\mathbf{B}$ obsahující jako bloky své sloupce. V terminologii předchozí věty tedy
$n = 1$ a $p =$ počet sloupců matice $\mathbf{B}$.

Věta ?? se dá lapidárně formulovat takto: sloupce maticového součinu
obsahují součiny celé matice $\mathbf{A}$ s odpovídajícími sloupci matice $\mathbf{B}$. Analog
lze dokázat, že řádky maticového součinu $\mathbf{A} \cdot \mathbf{B}$ obsahují součiny odpovídaj
řádků matice $\mathbf{A}$ s celou maticí $\mathbf{B}$. Tuto větu si přesně zforuluje již laskavý čt
sám.

Rozdělme v maticovém součinu $\mathbf{A} \cdot \mathbf{B}$ matici $\mathbf{A}$ na řádky a současně m
$\mathbf{B}$ na sloupce. Pak věta ?? nám říká, že každý prvek součinu $c_{i,k}$ se počítá
maticový součin i-tého řádku matice $\mathbf{A}$ s k-tým sloupcem matice $\mathbf{B}$. Ka
takový součin je roven sumě ve vzorci (??). Takže tímto pohledem nezísk
nic jiného, než přímo definici maticového násobení ??.

Jiný pohled na maticový součin z předchozí poznámky ilustrujeme na kladu ??. Matice vynásobíme tak, že první matici rozdělíme na sloupce a dru na řádky. Dostáváme

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 0 & 2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \\ 2 & 7 \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \end{pmatrix} + \begin{pmatrix} 2 \\ 6 \\ 2 \end{pmatrix} \cdot \begin{pmatrix} 3 & 4 \end{pmatrix} + \begin{pmatrix} 3 \\ 7 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 5 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 \\ 5 & 10 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 6 & 8 \\ 18 & 24 \\ 6 & 8 \end{pmatrix} + \begin{pmatrix} 15 & 18 \\ 35 & 42 \\ 5 & 6 \end{pmatrix} + \begin{pmatrix} 8 & 28 \\ 16 & 56 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 30 & 56 \\ 74 & 132 \\ 11 & 14 \end{pmatrix}$$

Máme za úkol vynásobit dvě čtvercové matice z $\mathbf{R}^{n,n}$. Jak je to výpoč náročné? Předpokládejme, že násobení čísel je podstatně „dražší“ operace sčítání, takže se zaměříme na počet potřebných násobení dvou čísel a p sčítání budeme zanedbávat.

Pokud budeme postupovat při násobení čvercových matic podle definic budeme potřebovat pro výpočet každého prvku výsledku n operací a těch pr je n^2, takže dohoromady potřebujeme n^3 operací násobení. Lze na tom n ušetřit? V následujícím textu ukážeme, že ano, pokud použijeme rekurz blokový přístup k násobení matic. Uvedeme nejprve klasickou rekurzi pro sobení a následně tzv. *Strassenův algoritmus*, který rozšiřuje klasickou rek a ušetří operace.

(klasická rekurze) [klasrek] Předpokládejme, že násobíme čtvercové ma $\mathbf{A}$ a $\mathbf{B}$ z $\mathbf{R}^n$ a že navíc existuje přirozené m tak, že $n = 2^m$. Jinými sl každou matici lze rozkájet na čtyři čtvercové bloky stejně velké a tyto bloky znovu takto rozkrájet až na úroveň matic typu $(1, 1)$. Jak se zachovat, po tento předpoklad není splněn, je zmíněno v poznámce ??.

Proveďme výše zmíněné rozdělení matic $\mathbf{A}$ a $\mathbf{B}$ do bloků a použ nechat pokračovat až na úroveň bloků z $\mathbf{R}^{1,1}$ a teprve v tom případě násob odpovídající čísla mezi sebou.

Kolik potřebuje klasická rekurze operací násobení čísel? Je-li $F(n)$ p potřebných operací pro výpočet součinu matic z $\mathbf{R}^{n,n}$, kde $n = 2^m$, pak p

$$F(n) = 8F(n/2) = 8(8F(n/4)) = 8(8(8F(n/2^3))) = \cdots = 8^m F(n/2^m) = 8$$
$$= 8^m = (2^3)^m = 2^{3m} = (2^m)^3 = n^3.$$

Potřebujeme tedy stejný počet operací, jako kdybychom použili definici.

(Strassen) [strassen] Nechť dvě čtvercové matice $\mathbf{A}$ a $\mathbf{B}$ z $\mathbf{R}^{n,n}$ spl stejné předpoklady, jako v předchozím algoritmu, tj. $n = 2^m$ a rozdělme ma $\mathbf{A}$, $\mathbf{B}$ do bloků, jako před chvílí. Vypočteme pomocné matice:

$$\mathbf{X}_1 = (\mathbf{A}_1 + \mathbf{A}_4) \cdot (\mathbf{B}_1 + \mathbf{B}_4), \quad \mathbf{X}_2 = (\mathbf{A}_3 + \mathbf{A}_4) \cdot \mathbf{B}_1, \quad \mathbf{X}_3 = \mathbf{A}_1 \cdot (\mathbf{B}_2 -$$
$$\mathbf{X}_5 = (\mathbf{A}_1 + \mathbf{A}_2) \cdot \mathbf{B}_4, \quad \mathbf{X}_6 = (\mathbf{A}_3 - \mathbf{A}_1) \cdot (\mathbf{B}_1 + \mathbf{B}_2), \quad \mathbf{X}_7 = (\mathbf{A}_2 - \mathbf{A}_4)$$

Čtenář si jako cvičení ověří, že platí:

$$\begin{pmatrix} \mathbf{A}_1 & \mathbf{A}_2 \\ \mathbf{A}_3 & \mathbf{A}_4 \end{pmatrix} \cdot \begin{pmatrix} \mathbf{B}_1 & \mathbf{B}_2 \\ \mathbf{B}_3 & \mathbf{B}_4 \end{pmatrix} = \Bigg(\begin{matrix} \mathbf{X}_1 + \mathbf{X}_4 - \mathbf{X}_5 + \mathbf{X}_7 & \mathbf{X}_3 + \mathbf{X}_5 \\ \mathbf{X}_2 + \mathbf{X}_4 & \mathbf{X}_1 - \mathbf{X}_2 + \mathbf{X}_3 + \mathbf{X} \end{matrix}$$

Povšimneme si, že nyní jsme potřebovali pouze sedm maticových násob takže voláme rekurzivně sebe sama jen sedmkrát.

Kolik potřebujeme ve Strassenově algoritmu operací násobení jednotliv čísel? Předpokládejme matice z $\mathbf{R}^{n,n}$ a $n = 2^m$, neboli $m = \log_2 n$. Nechť F je počet operací násobení použitých ve Strassenově algoritmu, který sesta součin matic z $\mathbf{R}^{n,n}$. Pak

$$F(n) = 7F(n/2) = 7(7F(n/4)) = 7(7(7F(n/2^3))) = \cdots = 7^m F(n/2^m) = 7$$

V článku [7] Don Coppersmith a Shmuel Winograd uvádějí algorit který má ještě lepší složitost: $n^{2,376}$, ovšem přidává tolik dodatečných režij operací a paměťových nároků, že by byl užitečný jen pro tak rozsáhlé ma které se v současné době nevejdou do počítače. Používá se tedy jen jako te tická dosud známá nejlepší mez složitosti pro maticové násobení. Dosud při není dokázáno, jaká je skutečná nejlepší mez, tj. zda by bylo možné toto ještě vylepšit.

[rekurzeruznych] Pokud násobíme matice, které nejsou čvercové nebo ne typu $(2^m, 2^m)$, pak je potřeba rozšířit matice o nulové řádky nebo sloupce obojí tak, aby rozšířené matice byly typu $(2^m, 2^m)$. Pak je možné použít uvedené rekurzivní algoritmy. V nich můžeme hlídat rozsah indexů jednotli bloků a pokud je celý blok v prostoru, kde jsou jen nuly, nemusí algorit součin počítat a rovnou vrátí jako výsledek nulový blok. Je to pouze techn vychytávka výše popsaných algoritmů, která neovlivní teoretické výsledk kterých jsme se zmínili dříve. Ve výsledku je pak potřeba zpětně odebrat šířující řádky a sloupce (které stejně vyjdou nulové).

Nechť je dána čtvercová matice $\mathbf{A} \in \mathbf{R}^{n,n}$. Pokud matice $\mathbf{B}$ splňuje rov $\mathbf{A} \cdot \mathbf{B} = \mathbf{B} \cdot \mathbf{A}$, říkáme, že matice $\mathbf{B}$ *komutuje* s maticí $\mathbf{A}$.

Zabývejme se vlastnostmi matic $\mathbf{B}$, které komutují s pevně danou čt covou maticí $\mathbf{A} \in \mathbf{R}^{n,n}$. Například matice $\mathbf{A}$ komutuje sama se sebou, n součin $\mathbf{A} \cdot \mathbf{A}$ je pro čtvercovou matici definován a prohození činitelů v nepoznáme.

Matice $\mathbf{B}$ komutující s $\mathbf{A}$ musí mít stejný počet řádků jako matic sloupců (aby bylo definováno $\mathbf{A} \cdot \mathbf{B}$) a také musí mít stejný počet sloupců matice $\mathbf{A}$ řádků (aby bylo definováno $\mathbf{B} \cdot \mathbf{A}$). To prakticky znamená, že ma $\mathbf{B}$ musí být také čtvercová, typu (n, n).

Z příkladu ?? víme, že ne všechny matice z $\mathbf{R}^{n,n}$ komutují s danou čt použijeme věty ??, vzorce (2) až (4) a našeho předpokladu.

$$\mathbf{A}\cdot(\mathbf{B}+\mathbf{C})=\mathbf{A}\cdot\mathbf{B}+\mathbf{A}\cdot\mathbf{C}=\mathbf{B}\cdot\mathbf{A}+\mathbf{C}\cdot\mathbf{A}=(\mathbf{B}+\mathbf{C})\cdot\mathbf{A},$$
$$\mathbf{A}\cdot(\alpha\,\mathbf{B})=\alpha\,(\mathbf{A}\cdot\mathbf{B})=\alpha\,(\mathbf{B}\cdot\mathbf{A})=(\alpha\,\mathbf{B})\cdot\mathbf{A}.$$

[basekomut] Najdeme bázi a dimenzi lineárního podprostoru M všech
tic komutujících s maticí

$$\mathbf{A}=\begin{pmatrix}1&2\\3&4\end{pmatrix}.$$

Podle předchozího příkladu musejí být matice komutující s maticí $\mathbf{A}$ ro
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

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}\cdot\begin{pmatrix}1&2\\3&4\end{pmatrix}=\begin{pmatrix}a+3b&2a+4b\\c+3d&2c+4d\end{pmatrix},\quad\begin{pmatrix}1&2\\3&4\end{pmatrix}\cdot\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{pmatrix}a+2\\3a+4\end{pmatrix}$$

Tyto součiny se mají rovnat. Podle poznámky ?? se dvě matice rovnají,
kud se vzájemně rovnají všechny jejich odpovídající prvky. To nás ved
čtyřem rovnicím o čtyřech neznámých, které upravíme Gaussovou elminin
metodou.

$$\begin{aligned}3b-2c&=0\\2a+3b-2d&=0\\-3a-3c+3d&=0\\-3b+2c&=0\end{aligned}\qquad\begin{pmatrix}0&3&-2&0\\2&3&0&-2\\-1&0&-1&1\\0&-3&2&0\end{pmatrix}\sim\begin{pmatrix}2&3&0&-2\\0&3&-2&0\end{pmatrix}$$

Lineární prostor všech komutujících matic M se nám podařilo vyjádřit
množinu všech lineárních kombinací dvou konstantních matic. Tuto skuteč
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, po
se spokojíme se zlomkem ve výsledku. V modelových příkladech se dosti č
snažíme dostat výsledek vyjádřitelný v malých celých číslech. Není to sa
zřejmě naší povinností, pouze pak výsledek lépe vypadá a nás více potěší.

Protože poslední dvě uvedené matice jsou lineárně nezávislé (to sna
zjistíme) a jejich lineární obal je celý podprostor M, máme výsledek:

$$\text{Báze } M = \left\{ \begin{pmatrix} -3 & 2 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}, \quad \text{tj. } \dim M = 2.$$

[matvektoru] V definici ?? jsme zavedli matice, jejíž prvky jsou re
nebo komplexní čísla. Občas se můžeme setkat s maticemi, jejíž prvky
vektory, tedy prvky libovolného lineárního prostoru. Protože lze prvky lin
ního prostoru podle definice ?? násobit reálným číslem, lze přirozeně defin
též maticové násobení $\mathbf{A} \cdot \mathbf{B}$, kde $\mathbf{A} = (a_{i,j}) \in \mathbf{R}^{m,n}$ je matice reálných čís
$\mathbf{B} = (\boldsymbol{b}_{j,k})$ je matice typu (n, p) obsahující vektory lineárního prostoru L,
$\mathbf{B} \in L^{n,p}$. Výsledná matice $\mathbf{A} \cdot \mathbf{B}$ je z množiny $L^{m,p}$ a pro její prvky $\boldsymbol{c}_{i,k}$ p

$$\boldsymbol{c}_{i,k} = a_{i,1}\, \boldsymbol{b}_{1,k} + a_{i,2}\, \boldsymbol{b}_{2,k} + \cdots + a_{i,n}\, \boldsymbol{b}_{n,k} = \sum_{j=1}^{n} a_{i,j}\, \boldsymbol{b}_{j,k}.$$

Nechť $\mathbf{A} \in \mathbf{R}^{1,n}$ je matice reálných čísel a $\mathbf{B} \in L^{n,1}$ Pak součin $\mathbf{A}$

* [ABlkB] Předchozí příklad nám poskytuje další pohled na maticové
sobení. Předpokládejme matice $\mathbf{A} \in \mathbf{R}^{m,n}$, $\mathbf{B} \in \mathbf{R}^{n,p}$, $\mathbf{C} = \mathbf{A} \cdot \mathbf{B} \in \mathbf{R}$
Na matici $\mathbf{B}$ se dívejme jako na jednosloupcovou matici jejích řádků. P
řádek výsledné matice $\mathbf{C}$ obsahuje lineární kombinaci řádků matice $\mathbf{B}$, přič
koeficienty této lineární kombince jsou v prvním řádku matice $\mathbf{A}$. Také ka
k-tý řádek matice $\mathbf{C}$ obsahuje lineární kombinaci všech řádků matice $\mathbf{B}$ a
koeficienty jsou v k-tém řádku matice $\mathbf{A}$.

* [hodA.B] Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$, $\mathbf{B} \in \mathbf{R}^{n,p}$. Pak $\operatorname{hod}(\mathbf{A} \cdot \mathbf{B}) \le \operatorname{hod} \mathbf{A}$ a
$\operatorname{hod}(\mathbf{A} \cdot \mathbf{B}) \le \operatorname{hod} \mathbf{B}$. Jinými slovy: hodnost maticového součinu není větší
hodnosti jednotlivých činitelů.

Důkaz. Podle poznámky ?? víme, že řádky matice $\mathbf{AB}$ jsou lineárními ko
nacemi řádků matice $\mathbf{B}$. Takže $\mathrm{r}\colon \mathbf{AB} \subseteq \langle \mathrm{r}\colon \mathbf{B} \rangle$, tj. $\langle \mathrm{r}\colon \mathbf{AB} \rangle \subseteq \langle \langle \mathrm{r}\colon \mathbf{B} \rangle \rangle = \langle \mathrm{r}$
Podle věty ?? tedy je $\dim \langle \mathrm{r}\colon \mathbf{AB} \rangle \le \dim \langle \mathrm{r}\colon \mathbf{B} \rangle$, neboli $\operatorname{hod}(\mathbf{A} \cdot \mathbf{B}) \le \operatorname{hod} \mathbf{B}$

Protože platí věty ?? a ??, můžeme psát $\operatorname{hod}(\mathbf{A} \cdot \mathbf{B}) = \operatorname{hod}(\mathbf{A} \cdot \mathbf{B})$
$\operatorname{hod}(\mathbf{B}^T \cdot \mathbf{A}^T)$ a z právě dokázané nerovnosti plyne, že $\operatorname{hod}(\mathbf{B}^T \cdot \mathbf{A}^T) \le \operatorname{hod} \mathbf{A}$
$\operatorname{hod} \mathbf{A}$. Dokázali jsme $\operatorname{hod}(\mathbf{A} \cdot \mathbf{B}) \le \operatorname{hod} \mathbf{A}$.

[defE] Čtvercovou matici $\mathbf{E} \in \mathbf{R}^{n,n}$ nazýváme *jednotkovou maticí*, po
pro její prvky $e_{i,j}$ platí: $e_{i,j} = 0$ pro $i \ne j$ a $e_{i,j} = 1$ pro $i = j$. Názorně:

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

[poznE] Z definice maticového násobení okamžitě plyne, že pro kaž
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 t
stejnou vlastnost vzhledem k násobení, jako jednička při násobení reáln

báze lineárního podprostoru M je $\{\mathbf{A}, \mathbf{E}\}$. Zdálo by se, že jsme výpočty v
kladu ?? dělali zbytečně. Není to tak docela pravda, protože dopředu nev
zda dimenze hledaného prostoru bude rovna dvěma.

V definici ?? jsme zavedli jednotkovou matici s podobnými vlastnos
jako má reálné číslo 1. Vraťme se znovu ke srovnání s reálnými čísly. Pro ka
nenulové reálné číslo a existuje reálné číslo b takové, že $ab = 1$. Takové re
číslo obvykle nazýváme převrácenou hodnotou čísla a a označujeme $1/a$ n
též a^{-1}. Analogicky definujeme „převrácenou hodnotu matice“, tzv. inve
matici.

* [inverseA] Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$ je čtvercová matice a $\mathbf{E} \in \mathbf{R}^{n,n}$ je jednot
matice. Matici $\mathbf{B} \in \mathbf{R}^{n,n}$, která splňuje vlastnost $\mathbf{A} \cdot \mathbf{B} = \mathbf{E} = \mathbf{B} \cdot \mathbf{A}$ nazýv
inverzní maticí k matici $\mathbf{A}$. Inverzní matici k matici $\mathbf{A}$ označujeme symbo
$\mathbf{A}^{-1}$.

[jedinainv] Pokud k matici $\mathbf{A}$ existuje inverzní matice, pak je tato inve
matice jednoznačně určena.

Důkaz. Nechť má čtvercová matice $\mathbf{A}$ dvě inverzní matice $\mathbf{B}$ a $\mathbf{C}$. Ukáže
že pak $\mathbf{B} = \mathbf{C}$. Platí:

$$\mathbf{B} = \mathbf{B} \cdot \mathbf{E} = \mathbf{B} \cdot (\mathbf{A} \cdot \mathbf{C}) = (\mathbf{B} \cdot \mathbf{A}) \cdot \mathbf{C} = \mathbf{E} \cdot \mathbf{C} = \mathbf{C}.(B = C)$$

Zde jsme po řadě využili: poznámku ??, vlastnost, že $\mathbf{C}$ je inverzní matice
vlastnost (1) z věty ??, vlastnost, že $\mathbf{B}$ je inverzní matice k $\mathbf{A}$, a konečně zn
poznámku ??.

* [dregul] Čtvercová matice $\mathbf{A} \in \mathbf{R}^{n,n}$ se nazývá *regulární*, pokud
$\mathbf{A}$ existuje inverzní matice. Čtvercová matice $\mathbf{A} \in \mathbf{R}^{n,n}$ se nazývá *singul*
pokud není regulární.

[hodreg] Matice $\mathbf{A}$ je regulární právě když hod $\mathbf{A} = n$, kde n je počet řá
matice $\mathbf{A}$.

Protože hod $\mathbf{A}$ = hod $\mathbf{A}^T$, jsou i sloupce matice $\mathbf{A}$ lineárně nezávislé a t bázi (B') lineárního prostoru $\mathbf{R}^n$. Souřadnice i-tého sloupce matice $\mathbf{E}$ vzhle k (B') napišme do i-tého sloupce matice $\mathbf{C}$. Zřejmě je $\mathbf{C}^T \cdot \mathbf{A}^T = \mathbf{E}$, ne $\mathbf{A} \cdot \mathbf{C} = \mathbf{E}^T = \mathbf{E}$. Z rovností $\mathbf{B} \cdot \mathbf{A} = \mathbf{E}$ a $\mathbf{A} \cdot \mathbf{C} = \mathbf{E}$ plyne $\mathbf{B} = \mathbf{C}$. Proč? S zopakovat výpočet (??), který jsme provedli v důkazu věty ??. Podle defi je $\mathbf{B}$ inverzní matice k matici $\mathbf{A}$. Matice $\mathbf{A}$ je tedy regulární.

[stacipul] Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$. Z existence matice $\mathbf{B}$ takové, že $\mathbf{B} \cdot \mathbf{A}$ = plyne, že $\mathbf{A}$ je regulární a $\mathbf{B}$ je její inverzní matice. Z existence matice $\mathbf{C}$ tak 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 ?? pl že $n = \text{hod}(\mathbf{B} \cdot \mathbf{A}) \le \text{hod}\,\mathbf{A}$, takže hod $\mathbf{A} = n$. Nyní sestavíme matici $\mathbf{C}$ ja předchozím důkazu a ukážeme, že $\mathbf{A} \cdot \mathbf{C} = \mathbf{E}$ a navíc $\mathbf{B} = \mathbf{C}$, takže je to inve matice k matici $\mathbf{A}$. Vyjdeme-li z existence matice $\mathbf{C}$, postupujeme obdobn

Předchozí věta říká, že v definici ?? je jedna z rovností $\mathbf{A} \cdot \mathbf{B} = \mathbf{E}$, $\mathbf{B} \cdot \mathbf{A}$ „nadbytečná“, protože z jedné rovnice plyne druhá a z druhé plyne první.

[regulkratregul] Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$ a $\mathbf{B} \in \mathbf{R}^{n,n}$ jsou regulární čtver 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 m cového součinu. Stačí tedy dokázat, že je regulární. Podle definice ?? je ma regulární právě tehdy, když k ní existuje inverzní matice. Podle předpok k matici $\mathbf{A}$ existuje inverzní matice $\mathbf{A}^{-1}$ a k matici $\mathbf{B}$ existuje inverzní ma $\mathbf{B}^{-1}$. Stačí ukázat, že existuje inverzní matice k matici $\mathbf{A} \cdot \mathbf{B}$. Hledaná inve matice je tvaru $\mathbf{B}^{-1} \cdot \mathbf{A}^{-1}$, protože:

$$(\mathbf{B}^{-1} \cdot \mathbf{A}^{-1}) \cdot (\mathbf{A} \cdot \mathbf{B}) = \mathbf{B}^{-1} \cdot (\mathbf{A}^{-1} \cdot \mathbf{A}) \cdot \mathbf{B} = \mathbf{B}^{-1} \cdot \mathbf{E} \cdot \mathbf{B} = \mathbf{B}^{-1} \cdot \mathbf{B} =$$

* [metodainverse] Na jednoduchém příkladu ukážeme obvyklý postup

Vedle prvků matice $\mathbf{A}$ napíšeme prvky jednotkové matice stejného typu (od
líme od sebe pro přehlednost svislou čarou) a dále použijeme řádkové úpr
Gaussovy eliminační metody na matici $(\mathbf{A}|\mathbf{E})$ jako celek. To znamená, že
cujeme s řádky délky $2n$, v našem konkrétním případě s řádky o šesti prvc
Při eliminaci se snažíme vlevo od svislé čáry dostat postupně jednotkovou
tici.

$$\left(\begin{array}{rrr|rrr} 1 & 2 & 3 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 & 1 & 0 \\ 2 & 2 & 1 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{rrr|rrr} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 2 & 4 & 1 & 1 & 0 \\ 0 & -2 & -5 & -2 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{rr} 1 & 2 \\ 0 & 2 \\ 0 & 0 \end{array}\right.$$

$$\sim \left(\begin{array}{rrr|rrr} 1 & 2 & 0 & -2 & 3 & 3 \\ 0 & 2 & 0 & -3 & 5 & 4 \\ 0 & 0 & 1 & 1 & -1 & -1 \end{array}\right) \sim \left(\begin{array}{rrr|rrr} 1 & 0 & 0 & 1 & -2 & -1 \\ 0 & 1 & 0 & -\frac{3}{2} & \frac{5}{2} & 2 \\ 0 & 0 & 1 & 1 & -1 & -1 \end{array}\right), \quad \mathbf{A}$$

Při přechodu z matice $\mathbf{A}$ na matici $\mathbf{E}$ v levém bloku jsme nejprve přev
matici $\mathbf{A}$ na schodovitou matici stejně, jako je popsáno v úvodní kapito
Gaussově eliminační metodě (tzv. *přímý chod eliminační metody*). Jsou-l
schodovité matici na diagonále nenulové prvky, lze pokračovat tzv. *zpět*
chodem eliminační metody. V něm nejprve násobíme poslední řádek vhodn
konstantami a přičítáme k řádkům nad ním. Tím dostáváme nuly v posled
sloupci nad nenulovým prvkem na pozici (n, n). Pak přičítáme násobky p
posledního řádku k předchozím a získáme nuly v předposledním sloupci. Ta
postupně pokračujeme až dostaneme matici s nenulovými prvky na diago
a s nulovými prvky jinde. Každý řádek takové matice vynásobíme převráce
hodnotou jeho diagonálního prvku a dostáváme matici $\mathbf{E}$.

Tvrdíme, že hledaná inverzní matice k matici $\mathbf{A}$ je zapsána vpravo
svislé čáry v poslední úpravě. Zformulujeme to jako algoritmus:

* [algolinverse] Pokud $(\mathbf{A}\,|\,\mathbf{E}) \sim (\mathbf{E}\,|\,\mathbf{B})$, kde „$\sim$“ znamená konečně mn
řádkových úprav matice podle Gaussovy eliminační metody, pak $\mathbf{B} = \mathbf{A}^{-1}$

Zvídavý čtenář se oprávněně ptá, proč tato metoda dává inverzní ma kombinací do řádků matice $\mathbf{P}$, dostáváme podle poznámky ?? vztah $\mathbf{P} \cdot \mathbf{A} =$

[inverse] Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$ a nechť lze provést $(\mathbf{A} \,|\, \mathbf{E}) \sim (\mathbf{E} \,|\, \mathbf{B})$, kde označuje konečný počet řádkových úprav podle eliminační metody a $\mathbf{E}$ z 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 ?? inverzní matice k matici $\mathbf{A}$.

[emulacesloupcu] Kdybychom napsali jednotkovou matici pod matic a aplikovali na sloupce této „dvojmatice“ sloupcové úpravy podle Gauss eliminační metody a získali nakonec v horní části matici $\mathbf{E}$, pak je ve spo části matice inverzní. Při důkazu tohoto tvrzení bychom postupovali analog jako při řádkové metodě, jen maticemi $\mathbf{P}_i$, které „emulují“ sloupcové úpr bychom násobili matici $\mathbf{A}$ zprava a nikoli zleva.

Rozmyslete si, že není možné při metodě hledání inverzní matice k binovat řádkové i sloupcové operace dohromady. Naráží to na skutečnost násobení matic není komutativní.

* [regulpodminky] Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$ je čtvercová matice. Pak následu podmínky jsou ekvivalentní:

(1) $\mathbf{A}$ je regulární,

(2) $\mathbf{A}$ má inverzní matici $\mathbf{A}^{-1}$,

(3) $\operatorname{hod} \mathbf{A} = n$,

(4) Maticová rovnice $\mathbf{AX} = \mathbf{B}$ s neznámou maticí $\mathbf{X} \in \mathbf{R}^{n,m}$ má řešení každou $\mathbf{B} \in \mathbf{R}^{n,m}$.

(5) $\mathbf{A} \sim \mathbf{E}$, tj. existuje konečně kroků Gaussovy eliminační metody, které vedou $\mathbf{A}$ na $\mathbf{E}$.

(4) $\Rightarrow$ (3): Je-li $\mathbf{C}$ řešení rovnice $\mathbf{AX} = \mathbf{E}$, pak musí podle věty ??
$\operatorname{hod} \mathbf{E} = \operatorname{hod}(\mathbf{A} \cdot \mathbf{C}) \le \operatorname{hod} \mathbf{A}$. Protože $\operatorname{hod} \mathbf{E} = n$, musí $\operatorname{hod} \mathbf{A} = n$.

(3) $\Rightarrow$ (5): Protože eliminace nemění hodnost, musí se po přímém ch
Gaussovy eliminace matice $\mathbf{A}$ proměnit ve schodovitou matici s nenulov
řádky, tedy s nenulovými čísly na diagonále. Pak lze provést zpětný chod
minace 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 ??.

Další ekvivalentní podmínkou regularity matice $\mathbf{A}$ je lineární nezávis
jejích řádků (podle věty ??) což je ekvivalentní s lineární nezávislostí slou
(podle věty ??) a to je ekvivalentní s regularitou matice $\mathbf{A}^T$. V násled
kapitole si ještě ukážeme, že $\mathbf{A}$ je regulární právě tehdy, když má nenu
determinant (věta ??).

Pro singulární matice lze zformulovat analogické podmínky: $\mathbf{A}$ je sin
lární, právě když neexistuje inverzní matice, právě když $\mathbf{AX} = \mathbf{B}$ nemá ře
pro některé matice $\mathbf{B}$, právě když $\operatorname{hod} \mathbf{A} < n$, právě když $\mathbf{A}$ má lineárně
vislé řádky/sloupce, právě když $\mathbf{A}^T$ je singulární, právě když nelze $\mathbf{A}$ pře
na $\mathbf{E}$ konečně mnoha kroky Gaussovy eliminační metody, právě když má nu
determinant.

Protože podle věty ?? je matice $\mathbf{A}$ regulární právě tehdy, když $\mathbf{A}$ ~
máme zaručeno, že metoda výpočtu inverzní matice neselže pro žádnou
gulární matici. Jinými slovy, má-li matice inverzní matici, pak půjde pro
eliminaci $(\mathbf{A}|\mathbf{E}) \sim (\mathbf{E}|\mathbf{B})$, což je podmínkou ke spuštění algoritmu ??.

Maticové rovnice z podmínky (4) lze řešit „vynásobením obou stran rov
maticí $\mathbf{A}^{-1}$ zleva“. Tím se $\mathbf{AX} = \mathbf{B}$ převede na $\mathbf{X} = \mathbf{A}^{-1}\mathbf{B}$. Dále lze
maticové rovnice $\mathbf{XA} = \mathbf{B}$ (pro matice $\mathbf{X}, \mathbf{B} \in \mathbf{R}^{m,n}$) „vynásobením o
stran rovnice maticí $\mathbf{A}^{-1}$ zprava“. Tím dostáváme $\mathbf{X} = \mathbf{BA}^{-1}$. Situace je
podobná jako s číselnou linární rovnicí $ax = b$ jen s tím rozdílem, že mus
mít na paměti, že není splněn komuntativní zákon součinu matic, takže $\mathbf{A}$
nemusí být totéž jako $\mathbf{BA}^{-1}$.

Hledaná matice musí být čtvercová typu $(3,3)$, jinak by nebylo definov
sčítání. Rovnici postupně upravíme (dáváme si pozor na to, že nemusí p
komutativní zákon).

$$\mathbf{A}\cdot\mathbf{X}-\mathbf{X}=-4\,\mathbf{A} \quad \text{tj.} \quad \mathbf{A}\cdot\mathbf{X}-\mathbf{E}\cdot\mathbf{X}=-4\,\mathbf{A} \quad \text{tj.} \quad (\mathbf{A}-\mathbf{E})\cdot\mathbf{X}=-4$$

Pokud existuje matice $(\mathbf{A}-\mathbf{E})^{-1}$, pak po pronásobení obou stran rovnice t
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
psanou v příkladu ??). Nalezenou inverzní matici vynásobíme čtyřmi a nak
provedeme maticové násobení $4\,(\mathbf{A}-\mathbf{E})^{-1}\cdot\mathbf{A}$ podle definice. Níže uvádíme
notlivé mezivýpočty:

$$\mathbf{A}-\mathbf{E}=\begin{pmatrix}0&2&3\\-1&-1&1\\2&2&0\end{pmatrix},\quad (\mathbf{A}-\mathbf{E})^{-1}=\begin{pmatrix}-\frac{1}{2}&\frac{3}{2}&\frac{5}{4}\\\frac{1}{2}&-\frac{3}{2}&-\frac{3}{4}\\0&1&\frac{1}{2}\end{pmatrix},\quad 4\,(\mathbf{A}-\mathbf{E}$$

$$\mathbf{X}=-4\,(\mathbf{A}-\mathbf{E})^{-1}\cdot\mathbf{A}=-\begin{pmatrix}-2&6&5\\2&-6&-3\\0&4&2\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\-1&0&1\\2&2&1\end{pmatrix}=\begin{pmatrix}-2&-6\\-2&2\\0&-4\end{pmatrix}$$

Z věty ?? víme, že hodnost matice se může zmenšit, pokud ji vynáso
nějakou maticí. Nyní ukážeme, že hodnost matice se nezmění, pokud ji vyn
bíme regulární maticí. Připomeneme nejdříve větu ??, která říká, že každ
eliminačnímu procesu $\mathbf{A}\sim\mathbf{B}$ přísluší matice $\mathbf{P}$ tak, že $\mathbf{B}=\mathbf{P}\cdot\mathbf{A}$. Tato
se dá v jistém smyslu obrátit:

[hodPA] Nechť $\mathbf{A}$ je libovolná matice (ne nutně čtvercová) a $\mathbf{P}$, $\mathbf{Q}$ regulární matice takové, že je definováno násobení $\mathbf{P} \cdot \mathbf{A}$ a $\mathbf{A} \cdot \mathbf{Q}$. Pak hod hod$(\mathbf{P} \cdot \mathbf{A}) = $ hod$(\mathbf{A} \cdot \mathbf{Q})$. Jinými slovy: násobení regulární maticí ne hodnost.

Důkaz. Označme $\mathbf{B} = \mathbf{P} \cdot \mathbf{A}$. Podle věty ?? je $\mathbf{A} \sim \mathbf{B}$, takže hod $\mathbf{A} = $ ho podle věty ??.

K důkazu hod $\mathbf{A} = $ hod$(\mathbf{A} \cdot \mathbf{Q})$ stačí podle (5) věty ?? přejít k transpo vaným 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 $\mathbf{A}$.

[AsimBequiv] $\mathbf{A} \sim \mathbf{B}$ 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 stavci ??. Nyní tedy předpokládáme $\langle \mathrm{r}\colon \mathbf{A} \rangle = \langle \mathrm{r}\colon \mathbf{B} \rangle$ a najdeme takový el nační proces, který převede matici $\mathbf{A}$ na matici $\mathbf{B}$.

Nejprve najdeme schodovité matice s nenulovými řádky $\mathbf{A}'$ a $\mathbf{B}'$ tak že $\mathbf{A} \sim \mathbf{A}'$ a $\mathbf{B} \sim \mathbf{B}'$. To je možné díky větě ??. Stačí tedy ukázat, že $\mathbf{A}' \sim$ 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 $\langle \mathrm{r}\colon \mathbf{A}$ $\langle \mathrm{r}\colon \mathbf{B} \rangle$ plyne $\langle \mathrm{r}\colon \mathbf{A}' \rangle = \langle \mathrm{r}\colon \mathbf{B}' \rangle$. Matice $\mathbf{A}'$ i $\mathbf{B}'$ mají lineárně nezávislé řád jejich počet je v obou případech roven $k = $ hod $\mathbf{A} = $ hod $\mathbf{B} = $ hod $\mathbf{A}' = $ ho Každý řádek matice $\mathbf{B}'$ je lineární kombinací řádků matice $\mathbf{A}'$, takže exis čtvercová matice $\mathbf{P}$ (koeficientů těchto lineárních kombinací), pro ktero $\mathbf{P} \cdot \mathbf{A}' = \mathbf{B}'$. Z věty ?? plyne, že hod $\mathbf{P} = k$, což je počet řádků matice $\mathbf{P}$. T $\mathbf{P}$ je podle věty ?? regulární. Po použití věty ?? vidíme, že $\mathbf{A}' \sim \mathbf{B}'$.

* [P123] Jestliže $\mathbf{A} \sim \mathbf{B}$, pak podle věty ?? existuje matice $\mathbf{P}$ takov $\mathbf{B} = \mathbf{P}\mathbf{A}$. Podívejme se, jak vypadá matice $\mathbf{P}$ v případě jednotlivých ele tárních kroků Gaussovy eliminační metody.

(1) Nechť $\mathbf{B}$ vznikla z $\mathbf{A}$ prohozením i-tého řádku s j-tým. Snadno ověř že $\mathbf{B} = \mathbf{P}_1 \cdot \mathbf{A}$, kde $\mathbf{P}_1$ je čtvercová matice, která vznikla z $\mathbf{E}$ prohozením i

[delement] Matice typu $\mathbf{P}_1$, $\mathbf{P}_2$ a $\mathbf{P}_3$ z příkladu ?? se nazývají *element matice*.

[BsimPA] Symbolem $\mathbf{A} \sim \mathbf{B}$ v této větě značíme skutečnost, že matic vznikla z matice $\mathbf{A}$ konečně mnoha kroky Gaussovy eliminační metody, přič není dovolen krok vynechání nebo přidání nulového řádku. Platí: $\mathbf{A} \sim \mathbf{B}$ p 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 ?? ovšem potřeba důkaz věty projít znovu a uvědomit si, že nebylo nutné po krok vynechání nebo přidání nulového řádku. Nyní dokážeme opačnou im kaci. Předpokládejme, že $\mathbf{A} \sim \mathbf{B}$. Pak

$$\mathbf{B} = \mathbf{C}_m \cdot (\mathbf{C}_{k-1} \cdots (\mathbf{C}_2 \cdot (\mathbf{C}_1 \cdot \mathbf{A})) \cdots) = (\mathbf{C}_m \cdot \mathbf{C}_{k-1} \cdots \mathbf{C}_2 \cdot \mathbf{C}_1) \cdot \mathbf{A} = \mathbf{P}$$

kde $\mathbf{C}_k$ je elementární matice jednoho z typů $\mathbf{P}_1$, $\mathbf{P}_2$ a $\mathbf{P}_3$, která „emul provedení k-tého kroku eliminační metody. Jednotlivé elementární matice zřejmě regulární, protože mají lineárně nezávislé řádky. Matice $\mathbf{P}$, kter součinem těchto elementárních regulárních matic, je podle věty ?? regulár

V následujících odstavcích budeme pracovat se skupinou vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2$ L a další skupinou vektorů $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_m \in L$, která vznikne jejich lineár kombinacemi. Tedy

$$\boldsymbol{y}_1 = \alpha_{1,1}\boldsymbol{x}_1 + \cdots + \alpha_{1,n}\boldsymbol{x}_n, \quad \boldsymbol{y}_2 = \alpha_{2,1}\boldsymbol{x}_1 + \cdots + \alpha_{2,n}\boldsymbol{x}_n, \quad \ldots, \quad \boldsymbol{y}_m = \alpha_{m,1}$$

Tyto rovnosti lze v souladu s poznámkou ?? zapsat jako maticový součin

$$\begin{pmatrix} \boldsymbol{y}_1 \\ \boldsymbol{y}_2 \\ \vdots \end{pmatrix} = \mathbf{A} \cdot \begin{pmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \\ \vdots \end{pmatrix}, \quad \text{stručně } \mathbf{Y} = \mathbf{A} \cdot \mathbf{X},$$

$\mathbf{R}^n$ řádky matice $\mathbf{A}$ a nechť $\boldsymbol{b} = (\beta_1, \beta_2, \ldots, \beta_n)$ je nějaký vektor z $\mathbf{R}$
$\boldsymbol{z} = \beta_1\, \boldsymbol{y}_1 + \beta_2\, \boldsymbol{y}_2 + \cdots + \beta_m\, \boldsymbol{y}_m$. Pak platí
(1) $\boldsymbol{b} \in \langle \boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m \rangle$ právě tehdy, když $\boldsymbol{z} \in \langle \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_m \rangle$.
(2) Jsou-li $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ lineárně nezávislé v L, pak $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m$ jsou l
árně nezávislé v $\mathbf{R}^n$ právě tehdy, když $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_m$ jsou lineárně nezáv
v L.
(3) Jsou-li $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ lineárně nezávislé, pak $\dim\langle \boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m \rangle = \dim$
(4) Je-li $m = n$ a $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ jsou lineárně nezávislé, pak $\langle \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}$
$\langle \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_n \rangle$.

Důkaz. (1) Nechť $\boldsymbol{b} \in \langle \boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m \rangle$, tedy $\boldsymbol{b} = \gamma_1\, \boldsymbol{a}_1 + \gamma_2\, \boldsymbol{a}_2 + \cdots + \gamma_m$
tj. $\boldsymbol{b} = (\gamma_1, \gamma_2, \ldots, \gamma_m) \cdot \mathbf{A}$. Protože $\mathbf{A} \cdot \mathbf{X} = \mathbf{Y}$, je $(\gamma_1, \gamma_2, \ldots, \gamma_m) \cdot \mathbf{Y}$
$(\gamma_1, \gamma_2, \ldots, \gamma_m) \cdot \mathbf{A} \cdot \mathbf{X} = \boldsymbol{b} \cdot \mathbf{X} = \boldsymbol{z}$. Takže $\boldsymbol{z} \in \langle \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_m \rangle$ a line
kombinace vektorů $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_m$, která tvoří $\boldsymbol{z}$, má stejné koeficienty,
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 $\boldsymbol{z} = (\gamma_1, \gamma_2, \ldots, \gamma_m) \cdot \mathbf{Y}$. Pro
$\mathbf{A} \cdot \mathbf{X} = \mathbf{Y}$, musí být $\boldsymbol{b} \cdot \mathbf{X} = \boldsymbol{z} = (\gamma_1, \gamma_2, \ldots, \gamma_m) \cdot \mathbf{Y} = (\gamma_1, \gamma_2, \ldots, \gamma_m) \cdot \mathbf{A}$
takže je $\boldsymbol{b} = (\gamma_1, \gamma_2, \ldots, \gamma_m) \cdot \mathbf{A}$. Vektor $\boldsymbol{b}$ je tedy lineární kombinací řá
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. Označ
symbolem $\boldsymbol{o}$ nulový vektor v L a ukážeme, že lineární kombinace $(\gamma_1, \gamma_2, \ldots,$
$\mathbf{Y} = \boldsymbol{o}$ musí být pouze triviální. Při označení $\boldsymbol{b} = (\gamma_1, \gamma_2, \ldots, \gamma_m) \cdot \mathbf{A}$
$\boldsymbol{o} = (\gamma_1, \gamma_2, \ldots, \gamma_m) \cdot \mathbf{A} \cdot \mathbf{X} = \boldsymbol{b} \cdot \mathbf{X}$. Lineární kombinace vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots$
je zde rovna nulovému vektoru. Protože jsou vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ line
nezávislé, musí být tato kombinace triviální, neboli $\boldsymbol{b} = (0, 0, \ldots, 0)$. Je t
$(\gamma_1, \gamma_2, \ldots, \gamma_m) \cdot \mathbf{A} = (0, 0, \ldots, 0)$. Levá strana této rovnosti je lineární kom
nace řádků matice $\mathbf{A}$ s koeficienty γ_i, která je rovna nulovému řádku. Pro
jsou tyto řádky lineárně nezávislé, musí $\gamma_i = 0$ pro $i = 1, 2, \ldots, m$.

vektorů $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_m$. Z vlastnosti (2) plyne, že obě tyto podmnožiny m
být stejně početné.

(4) Protože $\mathbf{Y} = \mathbf{A} \cdot \mathbf{X}$, je $\langle \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_n \rangle \subseteq \langle \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \rangle$. Pro
$\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ jsou lineárně nezávislé, je matice $\mathbf{A}$ regulární, takže $\mathbf{X} = \mathbf{A}^{-1}$
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
inkluze a uvedené lineární obaly se rovnají.

* [XsimY] Řádky matice $\mathbf{A}$ ve větě ?? jsou koeficienty lineárních kom
nací, kterými měníme skupinu vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ na novou skupinu vek
$\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_m$. Speciálně, je-li $\mathbf{A}$ některá z elementárních matic $\mathbf{P}_1$, $\mathbf{P}_2$ a
z příkladu ??, pak je regulární a má tedy lineárně nezávislé řádky. Podle
předchozí věty to znamená, že lineární nezávislost skupiny vektorů se nezm
změnou jejich pořadí, vynásobením jednoho vektoru nenulovou konstantou,
čtením násobku vektoru k jinému nebo konečným opakováním těchto úk
Z vlastnosti (4) předchozí věty dále vyplývá, že uvedené modifikace sku
vektorů nezmění jejich lineární obal. To nám připomíná věty ?? a ??, ale
jsme pracovali jen s řádky matice, tedy s vektory z $\mathbf{R}^n$. Nyní říkáme t
o vektorech z libovolného lineárního prostoru L.

Součin matic $\mathbf{A} \cdot \mathbf{B}$ je definován /??/ jen pro matice, kde $\mathbf{A}$ má st
počet sloupců jako $\mathbf{B}$ řádků. Součin matic není obecně komutativní ani
čtvercové matice. Ovšem platí asociativní i distributivní zákon /??/.

Matice lze násobit i po blocích /??, ??/. Například součin matic $\mathbf{A}$
obsahuje ve sloupcích součiny matice $\mathbf{A}$ s jednotlivými sloupci matice $\mathbf{B}$ /

Blokovým násobením matic je inspirován Strassenův algoritmus, který
složitost pouze $n^{2,8}$, zatímco složitost maticového součinu podle definice je

Existuje skupina matic, která s pevně danou čtvercovou maticí komut
Tato skupina tvoří podprostor všech čtvercových matic.

Iverzní matice ke čtvercové matici $\mathbf{A}$ ja taková čtvercová matice $\mathbf{A}^{-1}$
ného typu, která musí splňovat $\mathbf{A} \cdot \mathbf{A}^{-1} = \mathbf{A}^{-1} \cdot \mathbf{A} = \mathbf{E}$ /??/, kde $\mathbf{E}$ je

Gaussově eliminační metodě. Že metoda skutečně počítá inverzní matici p
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 /??
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
torů z L k lineárním kombinacím této skupiny vektorů. Odvodili jsme, že
na abstraktní vektory z L můžeme uplatnit kroky Gaussovy eliminační met
jako na řádky matice, přitom jejich lineární nezávislost a jejich lineární
zůstávají v takovém případě zchovány /??/.

7. LU rozklad

V této krátké kapitole ukážeme, že každou regulární matici lze (až
případné prohození sloupců) zapsat jako součin matic **L** a **U**, kde **L** je d
trojúhelníková matice (má nenulové prvky soustředěny v dolním trojúheln
a **U** je horní trojúhelníková matice. Tento rozklad se používá při numeric
řešení soustav lineárních rovnic /??/, zejména při větším počtu pravých st

Toto téma spadá spíše do numerické matematiky. Přesto jsem se rozho
sem zařadit, protože hlavní myšlenka LU rozkladu využívá důležitý pozna
který byl vysloven v předchozí kapitole: jednotlivé kroky eliminační metody
„emulovat“ násobením příslušnými regulárními maticemi zleva. Následující
pitoly nepředpokládají znalosti o LU rozkladu. Pokud tedy čtenář nemá zá
tuto záležitost poznat hlouběji, může bez uzardění tuto kapitolu přeskočit

Nechť $\mathbf{A} = (a_{ij})$ je čtvercová matice. Matici **A** nazýváme *horní tr
helníkovou*, pokud má pod diagonálou jen nulové prvky (nenulové prvky
soustředěny v „horním tojúhelníku“), tedy $a_{i,j} = 0$ pro $i > j$. Matici **A** n
váme *dolní trojúhelníkovou*, pokud má nad diagonálou jen nulové prvky, t
$a_{i,j} = 0$ pro $i < j$.

[Linverz] (1) Součin dvou dolních trojúhelníkových matic s jedničkam
diagonále je dolní trojúhelníková matice s jedničkami na diagonále.
(2) Je-li **L** dolní trojúhelníková matice s jedničkami na diagonále, pak je r
lární 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 prov
takže **L** je regulární. $\mathbf{P} = \mathbf{L}^{-1}$ je součin elmentárních matic Gaussovy el
nace. Po přímém chodu Gaussovy eliminační metody jistě vytvoříme z d
trojúhelníkové matice **L** matici **E**. Zpětný chod není nutné použít, neboť

Matici $(\mathbf{A}\,|\,\mathbf{E})$ převedeme eliminací na $(\mathbf{U}\,|\,\mathbf{L}')$. Předpokládáme, že v el naci nejsme nuceni prohazovat řádky. Pouze přičítáme násobky řádků k řádl *pod nimi*. Tím máme zaručeno, že $\mathbf{L}'$ je dolní trojúhelníková matice s jed kami na diagonále.

Protože podle věty ?? existuje regulární čtvercová matice $\mathbf{P}$ taková, ž

$$(\mathbf{U}\,|\,\mathbf{L}') = \mathbf{P}\cdot(\mathbf{A}\,|\,\mathbf{E}) = (\mathbf{P}\cdot\mathbf{A}|\,\mathbf{P})$$

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 hleda matici $\mathbf{L}$ tedy platí $\mathbf{L} = (\mathbf{L}')^{-1}$. Matice $\mathbf{L}$ je podle věty ?? dolní trojúhelníl s jedničkami na diagonále.

[pLU] Platí

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 4 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 6 & 1 \end{pmatrix}\cdot\begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -5 \\ 0 & 0 & 18 \end{pmatrix} = \mathbf{LU},$$

protože

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 2 & 3 & 1 & 0 & 1 & 0 \\ 4 & 2 & 0 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -1 & -5 & -2 & 1 & 0 \\ 0 & 0 & 18 & 8 & -6 & 1 \end{array}\right) = (\mathbf{U}\,|\mathbf{L}'), \quad (\mathbf{L}$$

Pokud se při eliminaci použité v algoritmu ?? vyskytne na diagonál místě pivota) nulový prvek, jsme nuceni prohodit řádky nebo sloupce. V t vém případě matice $\mathbf{A}$ nemá přímý rozklad na $\mathbf{L}\cdot\mathbf{U}$. Místo toho rozklád modifikovanou matici $\mathbf{A}'$, která obsahuje vhodně přehozené řádky nebo slou matice $\mathbf{A}$ tak, aby k problému výskytu nulového diagonálního prvku bě eliminace nedošlo. Prohazování řádků lze emulovat násobením tzv.

Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$ je libovolná matice a $\mathbf{P} \in \mathbf{R}^{n,n}$ je permutační ma
Pak $\mathbf{PA}$ se liší od matice $\mathbf{A}$ jen prohozením některých řádků. Dále matice
se liší od matice $\mathbf{A}$ jen prohozením některých sloupců.

Důkaz. Jednotlivé elementární permutační matice prohazují při násobení z
dvojici řádků. Součin takových matic způsobí prohození více dvojic řádk
sebou, tedy nová matice $\mathbf{PA}$ má prohozeny některé řádky. Totéž platí pro so
$\mathbf{AP}$ a pro sloupce.

Pro permutační matici platí, že $\mathbf{P}^{-1} = \mathbf{P}^T$.

Důkaz. Stačí si uvědomit, že každá elementární permutační matice $\mathbf{P}$ má
denou vlastnost, tedy pro ni platí $\mathbf{P}^{-1} = \mathbf{P}^T$. Dokonce je $\mathbf{P} = \mathbf{P}^T = \mathbf{I}$
Nechť nyní $\mathbf{P} = \mathbf{C}_1\mathbf{C}_2 \cdots \mathbf{C}_k$, kde $\mathbf{C}_i$ jsou elementární permutační matice.

$$\mathbf{P}{\cdot}\mathbf{P}^T = (\mathbf{C}_1\mathbf{C}_2 \cdots \mathbf{C}_k)(\mathbf{C}_1\mathbf{C}_2 \cdots \mathbf{C}_k)^T = (\mathbf{C}_1\mathbf{C}_2 \cdots \mathbf{C}_k)(\mathbf{C}_k^T \cdots \mathbf{C}_2^T \cdots \mathbf{C}_1^T)$$

a analogicky $\mathbf{P}^T \cdot \mathbf{P} = \mathbf{E}$. je tedy $\mathbf{P}^{-1} = \mathbf{P}^T$.

[LUrozkladsloupce] Pro každou regulární matici $\mathbf{A} \in \mathbf{R}^{n,n}$ existuje
mutační matice $\mathbf{P} \in \mathbf{R}^{n,n}$, dolní trojúhelníková matice $\mathbf{L} \in \mathbf{R}^{n,n}$ s jedničk
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 naraz
na nulový diagonální prvek, pak v místě tohoto prvku nemůže být celý
dek nulový, protože matice $\mathbf{A}$ je regulární. Prohodíme v eliminované ma
sloupce tak, aby diagonální prvek byl nenulový. Toto prohození sloupc
možné podchytit maticovým násobením permutační matice zprava. Pro
řádkové eliminační úpravy lze podchytit násobením odpovídaícími matic
zleva, do součinu těchto matic se nám permutační matice „nemíchají“ a po
končení eliminace dostáváme $\mathbf{L}'\mathbf{AP} = \mathbf{U}$. Při označení $\mathbf{L} = (\mathbf{L}')^{-1}$ dostáv
$\mathbf{AP} = \mathbf{LU}$.

V tomto případě není matice $\mathbf{A}$ rozložitelná na součin $\mathbf{LU}$ bez předcho prohození jejích sloupců.

[LUrozkladradky] Pro každou regulární matici $\mathbf{A} \in \mathbf{R}^{n,n}$ existuje per tační matice $\mathbf{P} \in \mathbf{R}^{n,n}$, dolní trojúhelníková matice $\mathbf{L} \in \mathbf{R}^{n,n}$ s jedničkam 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 naraz na nulový diagonální prvek, pak pod tímto prvkem nemohou být samé n protože matice $\mathbf{A}$ je regulární. Prohodíme v eliminované matici řádky tak, diagonální prvek byl nenulový. Toto prohození řádků je možné podchytit m covým násobením permutační matice zleva. Protože řádkové eliminační úpr jsou podchyceny také násobením odpovídajícími maticemi zleva, bohužel, mutační matice se nám do součinu „přimíchaly“ a nemáme jistotu, že je mo je v součinu přesunout doprava bez porušení vlastnosti, že zbytek zůstane d diagonální matice. Pomůže ale následující představa. V okamžiku, kdy rozh neme o prohození řádků, se vátíme k původní matici $\mathbf{A}$ a prohodíme st řádky této matice. Pak eliminujeme znovu. Je zřejmé, že eliminace prob podobně, ale na nulový diagonální prvek už nyní nenarazíme. Pokračujen eliminaci dále. Narazíme-li později znovu na problém nulového prvku na agonále, prohodíme odpovídající řádky znovu v matici $\mathbf{A}$ a znovu elimi provedeme od začátku.

Pokud provádíme eliminaci celého bloku $(\mathbf{A}\,|\,\mathbf{E}) \sim (\mathbf{U}\,|\,\mathbf{L}')$, pak není n se po prohození řádků vracet na začátek eliminace, ale stačí prohodit v to bloku jen jisté části řádků. Přesněji. Nechť $a_{k,k} = 0$ a rozhodli jsme k-tý ř prohodit s $(k+j)$-tým. V dané chvíli je v pravém bloku v $(n+k)$-tém slo a ve všech dalších vrpavo od něj torzo ještě nezměněné jednotkové ma S tímto blokem při prohazování řádků nehýbeme, pouze prohodíme zkrá řádky délky $(n+k-1)$. Pak je možné rovnou v eliminaci pokračovat.

Najdeme LU rozklad matice $\mathbf{A}$ z příkladu ??

a poslední sloupec pravého bloku. Platí:

$$\mathbf{P} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \mathbf{L} = \begin{pmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ -2 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 4 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}, \quad \mathbf{U} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

Protože pro permutační matici $\mathbf{P}$ platí $\mathbf{P}^{-1} = \mathbf{P}^T$, což je také per tační matice, často se setkáváme s následujícími vzorci, které jsou důsle předchozích dvou vět:

$$\mathbf{A} = \mathbf{LUP}, \qquad \mathbf{A} = \mathbf{PLU}.$$

První vzorec je důsledkem eliminace s výběrem pivota prohazováním slou a druhý je důsledkem eliminace s výběrem pivota prohazováním řádků.

[jednoznacnostLU] Má-li matice $\mathbf{A} \in \mathbf{R}^{n,n}$ LU rozklad bez nutnosti hodit sloupce/řádky matice $\mathbf{A}$, je tento rozklad jednoznačný. Je-li nutné hodit sloupce/řádky v matici $\mathbf{A}$, pak pro každou možnou volbu proho sloupců/řádků je LU rozklad jednoznačný.

Důkaz. Nechť $\mathbf{A} = \mathbf{LU} = \mathbf{L}_1\mathbf{U}_1$, tj. předpokládáme dva LU rozklady ma $\mathbf{A}$. Protože je podle věty ?? matice $\mathbf{L}$ regulární, můžeme rovnost pronás 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 $\mathbf{L}^{-1}$ regulární, je regulární i matice $\mathbf{U}$, která je jejich součinem. Analogicky se vodí, že matice $\mathbf{U}_1$ je regulární, tedy má na diagonále nenulové prvky. po označení $\mathbf{L}^{-1}\mathbf{L}_1 = \mathbf{L}'$, což je podle věty ?? dolní trojúhelníková mati jedničkami na diagonále, dostáváme rovnost $\mathbf{U} = \mathbf{L}'\,\mathbf{U}_1$. Dá se ukázat pon věty ?? a přechodem k transponovaným maticím, že inverze horní trojúhe kové matice je horní trojúhelníková a že součin horních trojúhelníkových m

$\mathbf{L} = (\mathbf{L}')^{-1}$, ale využije se toho, že $\mathbf{L}$ obsahuje přímo koeficienty eliminac
opačným znaménkem).

Existují algoritmy LU rozkladu, které mají stejnou složitost jako matic
násobení. Takže při použití Strassenova algoritmu ?? máme složitost $n^{2,80}$

Regulární matici lze (až na prohození sloupců nebo řádků) zapsat jed
značně jako součin horní a dolní trojúhelníkové matice příslušných vlastn
/??, ??, ??, ??/.

8. Determinant

Determinant je číslo, které jistým způsobem charakterizuje čtvercovou
tici a které se využívá například při výpočtech řešení soustav lineárních ro
Toto číslo má mnoho důležitých významů, se kterými se setkáme nejen v
ární algebře, ale i v jiných matematických disciplínách. Determinant se p
definice počítá z prvků matice poměrně komplikovaným způsobem. Než
deme schopni tuto definici formulovat, musíme si něco říci o permutacích.
tomto pojmu je totiž definice determinantu založena.

[permutace] Nechť M je konečná množina o n prvcích. *Permutace p
množiny M* je uspořádaná n-tice prvků množiny M taková, že žádný p
z množiny M se v ní neopakuje. Permutaci prvků množiny $M = \{1, 2, \ldots$
nazýváme stručně *permutací n prvků*.

Uvedeme některé permutace pěti prvků: $(1, 2, 4, 5, 3)$, $(5, 4, 3, 2, 1)$, $(3, 5$
Uspořádanou pětici $(1, 2, 3, 2, 4)$ nepovažujeme za permutaci, protože se
opakuje prvek 2.

[pocetperm] Počet různých permutací n prvků je roven číslu $n!$.

Důkaz. Připomínáme, že $n! = n(n-1)(n-2)\cdots 2 \cdot 1$. Důkaz věty proved
matematickou indukcí. Pro čtenáře, který se s takovou formou důkazu j
nesetkal, nejprve vysvětlíme princip matematické indukce.

Matematickou indukcí dokazujeme tvrzení, které má platit pro všec
$n \in \mathbf{N}$. Postupujeme ve dvou krocích. Nejprve dokážeme toto tvrzení pro
1. Pak dokážeme tzv. indukční krok, který je formulován ve tvaru implik
„jestliže tvrzení platí pro n, pak platí pro $n + 1$“. Obhájíme-li platnost
implikace, máme dokázáno tvrzení pro všechna $n \in \mathbf{N}$. Vysvětlíme si, p
V prvním kroku jsme dokázali, že tvrzení platí pro $n = 1$. Uplatníme
indukční krok ve tvaru „jestliže tvrzení platí pro $n = 1$, pak platí pro $n =$

prvku je roven číslu $1! = 1$“. O tom ale asi nikdo nepochybuje, nelze t
vytvořit nic jiného než permutaci (1).

Nyní dokážeme indukční krok. Předpokládáme tedy, že počet různých
mutací n prvků je roven číslu $n!$ a dokážeme, že počet různých permutací n
prvků je roven číslu $(n+1)!$. Prozkoumejme nejprve, kolik existuje permu
$n+1$ prvků, které mají v první složce zapsáno číslo 1. Je jich $n!$, protože
lých n složek můžeme zaplnit čísly $\{2, 3, \ldots, n, n+1\}$ a máme v tomto příp
stejné množství možností, jako je počet permutací n prvků. Těch je podle
dukčního předpokladu $n!$. Ze stejného důvodu existuje $n!$ různých permu
$n+1$ prvků, které mají v první složce zapsáno číslo 2. Totéž platí pro
$3, 4, \ldots, n, n+1$ v první složce permutace. Existuje tedy $(n+1) \cdot n! = (n$
různých permutací $n+1$ prvků.

[ukazkaperm] Uvedeme si všechny permutace tří prvků. Podle věty ?
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.

$$(1,2,3,4),\ (1,2,4,3),\ (1,3,2,4),\ (1,3,4,2),\ (1,4,2,3),\ (1,4,3,2),\ (2,1,$$
$$(2,3,1,4),\ (2,3,4,1),\ (2,4,1,3),\ (2,4,3,1),\ (3,2,1,4),\ (3,2,4,1),\ (3,1,$$
$$(3,4,2,1),\ (3,4,1,2),\ (4,2,3,1),\ (4,2,1,3),\ (4,3,2,1),\ (4,3,1,2),\ (4,1,$$

Kdybychom chtěli zapsat všechny permutace 50 prvků, po použití věty
bychom si to rychle rozmysleli. Těch permutací totiž je přibližně $3 \cdot 10^{64}$. Kd
se nám na jeden řádek vešla jedna permutace a na stránku 60 řádků, spo
bovali bychom $5 \cdot 10^{62}$ stránek. Při oboustranném tisku váží 500 stránek
jeden kilogram, takže bychom spotřebovali 10^{57} tun papíru. Kdyby tisk je
stránky trval vteřinu, strávili bychom u tiskárny zhruba 10^{55} let. Jistě uzn
že to daleko přesahuje veškeré lidské možnosti.

Jako cvičení doplňte obloučky (tj. jednotlivé inverze) ke všem permutacím prvků.

[znper] Pro každou permutaci $\pi = (i_1, \ldots, i_n)$ definujeme *znaménko mutace* $\operatorname{sgn} \pi$ takto:

$$\operatorname{sgn} \pi = \begin{cases} +1 & \text{má-li } \pi \text{ sudý počet inverzí} \\ -1 & \text{má-li } \pi \text{ lichý počet inverzí} \end{cases}$$

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 pr

[prohperm] Prohození jediné dvojice prvků v permutaci způsobí zm jejího znaménka.

Důkaz. Nechť $\pi = (\ldots, a, \ldots, b, \ldots)$ a $\pi_1 = (\ldots, b, \ldots, a, \ldots)$ jsou dvě per tace, které se liší jen prohozením prvků a, b. Ukážeme, že rozdíl počtu inv permutací π a π_1 je liché číslo.

Inverze, ve kterých se nevyskytuje ani a, ani b, zůstávají v obou perm cích stejné. Tvoří-li dvojice (a, b) z permutace π inverzi, pak (b, a) z permu π_1 inverzi netvoří a naopak. Zatím jsme tedy zjistili, že se permutace π liší o jednu inverzi, což je liché číslo. Ještě prozkoumáme všechny inverze kterých vystupuje a nebo b s nějakým jiným prvkem. Ukážeme, že pokud dojde ke změně, pak jedině o sudý počet inverzí.

Uvažujme nějaký prvek x s menším indexem, než indexy prvků a i b, ně prvek y s větším indexem, než indexy prvků a i b a nějaký prvek z, který index mezi indexy a a b. Názorně:

Nechť nejprve $a < z < b$, tj. v permutaci π netvoří dvojice (a, z)
(z, b) inverzi. Pak v permutaci π_1 vznikají dvě nové inverze (b, z) a $(z, a$
to je sudé číslo. Nechť dále $b < z < a$, pak v permutaci π máme dvě inve
které v permutaci π_1 zanikají. Proběhla rovněž změna o sudý počet inv
Ještě může dojít k situaci $z < a$ a $z < b$. Pak v permutaci π dvojice (
tvoří inverzi a dvojice (z, b) netvoří, zatímco v permutaci π_1 dvojice (b, z) t
inverzi a dvojice (z, a) netvoří. Počet inverzí se tedy v tomto případě nezm
Poslední případ $a < z$ a $b < z$ ověříme podobně, jako předchozí.

[inverznip] Nechť $\pi = (i_1, i_2, \ldots, i_n)$ je permutace n prvků. *Inverzní*
mutací k permutaci π je permutace $(j_1, j_2, \ldots, j_n)$, pro kterou platí $j_{i_k} = k$
všechna $k \in \{1, 2, \ldots, n\}$. Tuto permutaci označujeme znakem π^{-1}.

[inverzniperm] Existuje několik možností, jak si představit inverzní per
taci k dané permutaci.

(1) Je-li v permutaci π na x-tém místě prvek y, pak v permutaci π^{-1}
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
vzestupně čísla $(1, 2, 3, \ldots, n)$. Pak ve spodním řádku je zapsána inverzní
mutace k permutaci π. Uvažujme kupříkladu permutaci $(3, 4, 2, 6, 1, 5)$ a piš

$$\begin{pmatrix} 3 & 4 & 2 & 6 & 1 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 2 & 6 & 4 \end{pmatrix}.$$

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 ša

sloupce, do druhé složky číslo řádku věže z druhého sloupce atd., dostáv
permutaci π^{-1}.

(4) Permutace $(i_1, i_2, \ldots, i_n)$ vymezuje zobrazení $\pi : \{1, 2, \ldots, n\} \to \{1$
pro které platí $\pi(k) = i_k$. Toto zobrazení je zjevně prosté a na mno
$\{1, 2, \ldots, n\}$. Inverzní zobrazení π^{-1} pak vymezuje inverzní permutaci.
$\pi \circ \pi^{-1} = \mathcal{I}$, kde $\mathcal{I}$ je identické zobrazení.

[inverzeinverzi] Nechť π je permutace n prvků. Pak π^{-1} má stejný p
inverzí, jako π.

Důkaz. Pro názornost si představíme inverzní permutaci způsobem (2) z
námky ??. Zaměřme se na dva sloupce uvedené dvouřádkové matice před
hozením sloupců:

$$\begin{pmatrix} \ldots, & x, & \ldots, & y, & \ldots \\ \ldots, & a, & \ldots, & b, & \ldots \end{pmatrix}.$$

Protože jde o stav před prohozením sloupců, víme, že $a < b$. Pokud x
tj. (x, y) netvoří inverzi v permutaci π, zůstanou po prohození sloupců
dva sloupce za sebou ve stejném pořadí. Takže se nová inverze v permu
π^{-1} nevytvoří. Pokud ale $x > y$, tj. (x, y) tvoří inverzi v permutaci π, pa
prohození sloupců budou tyto dva sloupce v opačném pořadí. Dvojice p
(b, a) tedy bude tvořit inverzi v permutaci π^{-1}.

[znpi-1] Permutace π a π^{-1} mají vždy stejná znaménka.

Důkaz. Věta je přímým důsledkem věty ??.

V předchozích definicích a větách jsme si řekli minimum toho, co potř
jeme vědět o permutacích, abychom pochopili definici determinantu a odv
jednoduché vlastnosti determinantu. Ve skutečnosti se u permutací dá stud
ještě mnoho dalších vlastností, které zde nebudeme potřebovat.

* [ddet] Nechť $\mathbf{A} = (a_{i,j}) \in \mathbf{R}^{n,n}$ je čtvercová matice. Číslo

Je možné, že vzorec z definice ?? je pro některé čtenáře málo srozumite
Pokusíme se jej proto v této poznámce trochu vysvětlit a zlidštit.

Představme si čtvercovou matici jako šachovnici rozměru $n \times n$ a poku
se na ni rozmístit n šachových věží tak, aby se vzájemně neohrožovaly. P
poznámky ??, odst. (3) je možné každé takové rozmístění popsat jednou
mutací (pozice věží čteme po řádcích). Podle věty ?? vidíme, že existuj
různých permutací, tedy existuje $n!$ různých řešení této šachové úlohy.
každé řešení této úlohy zapíšeme odpovídající permutaci, zjistíme zname
této permutace, nadzvedneme věžičky a zapíšeme si hodnoty prvků, na kter
ty figurky stojí, vynásobíme tyto hodnoty mezi sebou a výsledek ještě násob
znaménkem permutace. Pak si tento výsledek uložíme do paměti. Až projd
všech $n!$ možností rozmístění věží, získáme v paměti $n!$ sčítanců a ty sečte
Výsledkem je determinant matice.

[sarrus] 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. T
je podle věty ?? $3! = 6$. Zapíšeme všechny tyto permutace, jejich znamén
odpovídající rozmístění „šachových věží“.

$$\pi = (1,2,3), \quad \operatorname{sgn}\pi = +1, \quad \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}, \quad \text{sčítanec:} \quad +a_{1,1}\cdot$$

$$\pi = (2,3,1), \quad \operatorname{sgn}\pi = +1, \quad \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}, \quad \text{sčítanec:} \quad +a_{1,2}\cdot$$

$$\pi = (2,1,3), \quad \operatorname{sgn}\pi = -1, \quad \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}, \quad \text{sčítanec:} \quad -a_{1,2}\cdot$$

$$\pi = (1,3,2), \quad \operatorname{sgn}\pi = -1, \quad \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}, \quad \text{sčítanec:} \quad -a_{1,1}\cdot$$

$$\det \mathbf{A} = a_{1,1}\, a_{2,2}\, a_{3,3} + a_{1,2}\, a_{2,3}\, a_{3,1} + a_{1,3}\, a_{2,1}\, a_{3,2} - a_{1,3}\, a_{2,2}\, a_{3,1} - a_{1,2}\, a_{2,1}\, a_{3,}$$

Tento vzorec se dá zapamatovat pomocí mnemotechnické pomůcky: nej násobíme prvky na hlavní diagonále, dále ve směrech rovnoběžných s hl diagonálou a součiny sčítáme. Pak násobíme prvky na vedlejší diagonále, ve směrech rovnoběžných s vedlejší diagonálou, přičemž tyto součiny odečít Této „poučce o diagonálách“, která je použitelná jen pro matice typu (3 říkáme *Sarrusovo pravidlo*. Toto populární pravidlo tedy není nic jiného rozepsání definice determinantu pro matice z $\mathbf{R}^{3,3}$.

Pro matici typu $(4,4)$ bychom dostali při výpočtu determinantu podle finice $4! = 24$ sčítanců. Pro takovou matici se už těžko hledají mnemotechn pomůcky. Má-li čtenář čas a místo na papíře, může se pokusit sestavit všec permutace čtyř prvků, najít jejich znaménka a sečíst odpovídající součiny. kud čtenář nemá čas nebo místo na papíře, udělá nejlíp, když si počká na metodu na počítání determinantů, která bude vyžadovat daleko méně po ních úkonů. Na druhé straně rozepsání vzorce pro determinant matice t $(4,4)$ je užitečné cvičení pro pochopení definice determinantu.

[krizdet] Podobně, jako v předchozím příkladě, odvodíme vzorec pro počet determinantu matice z $\mathbf{R}^{2,2}$.

$$\pi = (1,2), \quad \operatorname{sgn}\pi = +1, \quad \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}, \quad \pi = (2,1), \quad \operatorname{sgn}\pi = -1,$$

prvek $a_{i,j}$, pro který platí $i > j$. *Prvek nad hlavní diagonálou* je každý p
$a_{i,j}$, pro který platí $i < j$.

[dettrojmatice] Nechť matice $\mathbf{A} \in \mathbf{R}^{n,n}$ má pod hlavní diagonálou
nulové prvky. Matice tedy názorně vypadá takto:

$$\mathbf{A} = \begin{pmatrix} a_{1,1}, & a_{1,2}, & \ldots, & a_{1,n-1}, & a_{1,n} \\ 0, & a_{2,2}, & \ldots, & a_{2,n-1}, & a_{2,n} \\ 0, & 0, & \ldots, & a_{3,n-1}, & a_{3,n} \\ & & \vdots & & \\ 0, & 0, & \ldots, & 0, & a_{n,n} \end{pmatrix} .(trojmatice)$$

Zkusíme spočítat det $\mathbf{A}$.

V definici determinantu ?? se pracuje se součtem součinů $\operatorname{sgn} \pi \cdot a$
$a_{2,i_2} \cdots a_{n,i_n}$. Pokud aspoň jeden z těchto činitelů je nulový, je nulový
součin. V celkovém součtu nás zajímají jen nenulové součiny. Prozkoume
které to jsou. Z posledního řádku musíme vzít jen prvek $a_{n,n}$, protože všec
ostatní prvky v posledním řádku jsou nulové. Z předposledního řádku můž
vzít jen prvek $a_{n-1,n-1}$, protože ostatní jsou nulové. Prvek $a_{n-1,n}$ nelze
součinu zahrnout, protože z posledního sloupce už v součinu máme prvek
(věže by se vzájemně ohrožovaly). Analogickou úvahou zahrneme do sou
prvky $a_{n-2,n-2}, \ldots, a_{2,2}, a_{1,1}$. Není tedy jiná možnost nenulového součinu,
součin $a_{1,1} \cdot a_{2,2} \cdots a_{n,n}$. Ten odpovídá permutaci $(1, 2, \ldots, n)$, která nemá
nou inverzi a její znaménko je tedy $+1$. Ostatní sčítanci z definice determina
jsou nuloví. Proto det $\mathbf{A} = a_{1,1} \cdot a_{2,2} \cdot a_{3,3} \cdots a_{n,n}$.

* [zvdet] Základní vlastnosti determinantu.

(V1) Jestliže se matice $\mathbf{B}$ liší od matice $\mathbf{A}$ jen prohozením jedné dvojice řá
pak det $\mathbf{B} = -$ det $\mathbf{A}$.

tečkami, se jednotlivé matice shodují.

$$\text{(V3)}\quad \det\begin{pmatrix}\vdots\\ \alpha\,\boldsymbol{a}_i\\ \vdots\end{pmatrix} = \alpha\det\begin{pmatrix}\vdots\\ \boldsymbol{a}_i\\ \vdots\end{pmatrix}.$$

$$\text{(V4)}\quad \det\begin{pmatrix}\vdots\\ \boldsymbol{a}_i\\ \vdots\end{pmatrix} + \det\begin{pmatrix}\vdots\\ \boldsymbol{b}_i\\ \vdots\end{pmatrix} = \det\begin{pmatrix}\vdots\\ \boldsymbol{a}_i+\boldsymbol{b}_i\\ \vdots\end{pmatrix}.$$

$$\text{(V5)}\quad \det\begin{pmatrix}\vdots\\ \boldsymbol{a}_i+\alpha\,\boldsymbol{a}_j\\ \vdots\end{pmatrix} = \det\begin{pmatrix}\vdots\\ \boldsymbol{a}_i\\ \vdots\end{pmatrix},\quad \text{kde } \boldsymbol{a}_j \text{ je nějaký jiný řádek téže}$$

Důkaz. (V1) Součin $a_{1,i_1}\cdots a_{n,i_n}$ odpovídá ve vzorci pro výpočet $\det\mathbf{A}$ mutaci $\pi = (i_1, i_2, \ldots, i_n)$. Tentýž součin najdeme i ve vzorci pro výpočet de pouze bude odpovídat permutaci π', která vznikne z permutace π přehoze dvou prvků. To podle věty ?? znamená, že $\operatorname{sgn}\pi' = -\operatorname{sgn}\pi$. V každém sčítanců pro výpočet $\det\mathbf{B}$ tedy máme opačné znaménko, než ve sčítancích 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, dostáv zase matici $\mathbf{A}$. Podle (V1) pro tuto matici platí $\det\mathbf{A} = -\det\mathbf{A}$, což nen být splněno jinak, než že $\det\mathbf{A} = 0$.

Vlastnosti (V3) a (V4) plynou přímo z definice determinantu:

(V5) dokážeme použitím právě dokázaných vlastností:

$$\det\begin{pmatrix}\vdots\\ \boldsymbol{a}_j\\ \vdots\\ \boldsymbol{a}_i+\alpha\,\boldsymbol{a}_j\\ \vdots\end{pmatrix} \overset{(V4)}{=} \det\begin{pmatrix}\vdots\\ \boldsymbol{a}_j\\ \vdots\\ \boldsymbol{a}_i\\ \vdots\end{pmatrix} + \det\begin{pmatrix}\vdots\\ \boldsymbol{a}_j\\ \vdots\\ \alpha\,\boldsymbol{a}_j\\ \vdots\end{pmatrix} \overset{(V3)}{=} \det\begin{pmatrix}\vdots\\ \boldsymbol{a}_j\\ \vdots\\ \boldsymbol{a}_i\\ \vdots\end{pmatrix} + \alpha\ \mathrm{de}$$

[metodadet] Vlastnosti (V1), (V3) a (V5) nám ukazují, jak se změní terminant, změníme-li matici pomocí Gaussovy eliminační metody. Proho řádků změní znaménko, vynásobení řádku nenulovým číslem α způsobí, ž determinant α-krát zvětší a konečně přičtení α-násobku jiného řádku ke lenému řádku nezmění hodnotu determinantu. Jsme tedy schopni uprav matice Gaussovou eliminační metodou, a přitom si poznamenávat, jak se n determinant. Tím můžeme převést matici na tvar (??). O této matici vím má determinant roven součinu prvků na hlavní diagonále.

Uvědomme si, že tato metoda dává výraznou úsporu času a výpočet prostředků při počítání determinantů. Představme si, že počítáme determi matice typu (n, n). Při Gaussově eliminační metodě potřebujeme zhruba n rací na výrobu jednoho nulového prvku. Těch nul potřebujeme vytvořit zh $n^2/2$, takže k výpočtu determinantu nám stačí $n^3/2$ operací. Pro matici $(50, 50)$ to je zhruba 62 500 operací. Pokud bychom chtěli počítat determi stejně velké matice přímo z definice, potřebovali bychom na to $50 \cdot 3 \cdot$ operací (viz komentář v příkladu ??). Není v silách žádné výpočetní tech spočítat to v rozumném čase.

[elimdet] Právě popsanou metodou spočítáme determinant matice

minant.

$$\begin{vmatrix} 1 & 2 & 4 & -1 \\ 2 & 1 & 2 & 2 \\ 1 & 3 & 1 & 2 \\ 2 & 1 & 2 & 1 \end{vmatrix} \overset{(1)}{=} \begin{vmatrix} 1 & 2 & 4 & -1 \\ 0 & -3 & -6 & 4 \\ 0 & 1 & -3 & 3 \\ 0 & -3 & -6 & 3 \end{vmatrix} \overset{(2)}{=} - \begin{vmatrix} 1 & 2 & 4 & -1 \\ 0 & 1 & -3 & 3 \\ 0 & -3 & -6 & 4 \\ 0 & -3 & -6 & 3 \end{vmatrix} \overset{(3)}{=} -$$

$$\overset{(4)}{=} - \begin{vmatrix} 1 & 2 & 4 & -1 \\ 0 & 1 & -3 & 3 \\ 0 & 0 & -15 & 13 \\ 0 & 0 & 0 & -1 \end{vmatrix} = -(-15) \cdot (-1) = -15.$$

V kroku (1) jsme první řádek násobili -2 a přičítali k druhému, pak jsme p řádek násobili -1 a přičítali k třetímu a nakonec jsme první řádek násobil a přičítali ke čtvrtému. Tyto operace podle (V5) nemění hodnotu deter nantu. V kroku (2) jsme prohodili druhý řádek se třetím, což podle (V1) zn znaménko determinantu. Napsali jsme toto znaménko před determinant difikované matice. V kroku (3) jsme druhý řádek násobili třemi a přičetl třetímu a čtvrtému. To podle (V5) nemění hodnotu determinantu. Kon v kroku (4) jsme třetí řádek násobili -1 a přičetli ke čtvrtému. Tím dostáv matici tvaru (??) z příkladu ??, o které víme, že má determinant roven sou prvků na diagonále.

Upozorňujeme na častou začátečnickou chybu při počítání determina V Gaussově eliminační metodě se většinou neklade důraz na to, který řá od kterého odečítáme, protože výsledný řádek můžeme kdykoli později nás číslem -1. Při počítání determinantů to ale jedno není. Například v kr (1) jsme od druhého řádku odečítali dvojnásobek prvního a výsledek psal druhý řádek. Kdybychom od dvojnásobku prvního řádku odečítali druh výsledek psali do druhého řádku, dopustili bychom se chyby, která nám zn znaménko determinantu. Mnemotechnická pomůcka: píšeme-li výsledek sou

Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$ má prvky na vedlejší diagonále rovny jedné a ost prvky jsou nulové. Spočítáme její determinant.

Prohodíme první řádek s posledním, druhý s předposledním atd. a dostaneme k prostřednímu řádku. Pro liché n necháváme prostřední řádek místě, pro sudé n prohodíme naposled mezi sebou řádky $n/2$ a $n/2+1$. V o případech jsme udělali $[n/2]$ prohození (symbolem $[x]$ zde značíme celou z x). Matici $\mathbf{A}$ jsme těmito úpravami převedli na jednotkovou matici $\mathbf{E}$. P předchozího příkladu je $\det \mathbf{E} = 1$, takže podle vlastnosti (V1) z věty ? $\det \mathbf{A} = (-1)^{[n/2]} \det \mathbf{E} = (-1)^{[n/2]}$.

Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$ má nad vedlejší diagonálou nulové prvky. Spočítáme determinant.

Prohazováním řádků, stejně jako v předchozím příkladě, převedeme ma na tvar (??). Prvky z vedlejší diagonály se při těchto úpravách přestěhuj hlavní diagonálu. Determinant takto upravené matice je podle příkladu ?? ro součinu prvků na diagonále, takže máme $\det \mathbf{A} = (-1)^{[n/2]} a_{1,n}\, a_{2,n-1} \cdots a$

[reguldet] Čtvercová matice $\mathbf{A}$ je regulární právě tehdy, když $\det \mathbf{A} \neq$

Důkaz. Všimneme si nejprve, že Gaussova eliminační metoda realizovaná k (V1), (V3) a (V5) podle předchozí věty ?? nemění „nulovost“ determina 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 Gau vou eliminační metodou na matici $\mathbf{B}$ tvaru (??) musejí být všechny prvky diagonále nenulové, protože podle věty ?? je také $\operatorname{hod} \mathbf{B} = n$. To znamená $\det \mathbf{B} \neq 0$ a tedy i $\det \mathbf{A} \neq 0$.

Je-li matice $\mathbf{A}$ singulární, je $\operatorname{hod} \mathbf{A} < n$. Po úpravě Gaussovou elimin metodou na matici $\mathbf{B}$ tvaru (??) bude existovat aspoň jeden řádek v ma $\mathbf{B}$ celý nulový. Nulový je tedy i diagonální prvek, takže $\det \mathbf{B} = 0$. P předchozího nutně musí být $\det \mathbf{A} = 0$.

* [det=detT] Nechť $\mathbf{A}$ je čtvercová matice. Pak $\det \mathbf{A} = \det \mathbf{A}^T$

činů, pouze permutace odpovídajících součinů je v prvním případě π a v
hém π^{-1}. Tyto permutace mají podle věty ?? stejný počet inverzí, takže i st
znaménko. Musí tedy být $\det \mathbf{A} = \det \mathbf{A}^T$.

Z právě dokázané věty plyne, že vlastnosti vyjmenované ve větě ?? p
nejen pro řádky matice, ale též pro sloupce. Při počítání determinantu p
metody popsané v poznámce ?? můžeme tedy svobodně přecházet od řádkov
úprav ke sloupcovým a zpět, protože vlastnosti (V1), (V3) a (V5) věty ?? p
nejen pro řádky, ale i pro sloupce (tzv. řádkově-sloupcová dualita).

* [rozvojdet] Nechť $\mathbf{A} = (a_{r,s}) \in \mathbf{R}^{n,n}$ je čtvercová matice a $\mathbf{A}_{i}$
$\mathbf{R}^{n-1,n-1}$ jsou matice, které vzniknou z matice $\mathbf{A}$ vynecháním i-tého řá
a j-tého sloupce. Pak pro každé $r \in \{1, \ldots, n\}$ platí

$$a_{r,1}\,(-1)^{r+1} \det \mathbf{A}_{r,1} + a_{r,2}\,(-1)^{r+2} \det \mathbf{A}_{r,2} + \cdots + a_{r,n}\,(-1)^{r+n} \det \mathbf{A}_{r,n} = \mathrm{d}$$

Je-li dále $t \in \{1, \ldots, n\}$, $t \neq r$, pak platí

$$a_{r,1}\,(-1)^{t+1} \det \mathbf{A}_{t,1} + a_{r,2}\,(-1)^{t+2} \det \mathbf{A}_{t,2} + \cdots + a_{r,n}\,(-1)^{t+n} \det \mathbf{A}_{t,n} = 0.($$

Důkaz (pro hloubavé čtenáře). Podívejme se na vzorec (??) pro $\det \mathbf{A}$. Se
píme v něm všechny sčítance, které obsahují prvek $a_{1,1}$ k sobě, dále seskup
k sobě sčítance, které obsahují prvek $a_{1,2}$ a tak dále až po poslední skupinu
které se vyskytují sčítanci s prvkem $a_{1,n}$. Tyto prvky ze součtů vytkneme.
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 $M = \{1, 2, \ldots, n\}$ vytvo
permutaci $\pi' = (i_2, \ldots, i_n)$ prvků množiny $M \setminus \{s\}$ tak, že odebereme p
prvek z permutace π. Nová permutace π' má o $s-1$ méně inverzí než permu

Determinant **A** je součtem všech skupin sčítanců pro $s = 1, 2, \ldots, n$, což d
zuje vzorec (??) pro $r = 1$.

Nechť nyní $r \neq 1$. Prohodíme r-tý řádek matice **A** s předchozím, pa
prohodíme s dalším předcházejícím řádkem, atd. až dostaneme původně
řádek na první řádek modifikované matice **B**. K tomu potřebujeme pro
$r-1$ prohození, takže platí $\det \mathbf{B} = (-1)^{r-1} \det \mathbf{A}$. Provedeme rozvoj dete
nantu matice **B** podle prvního řádku ($\mathbf{B}_{1,s}$ je matice, která vznikne z ma
B vynecháním prvního řádku a s-tého sloupce):

$$\det \mathbf{B} = a_{r,1}\,(-1)^{1+1} \det \mathbf{B}_{1,1} + a_{r,2}\,(-1)^{2+1} \det \mathbf{B}_{1,2} + \cdots + a_{r,n}\,(-1)^{1+n} \det \mathbf{}$$

Protože $\det \mathbf{A} = (-1)^{r-1} \det \mathbf{B}$ a protože $\mathbf{B}_{1,s} = \mathbf{A}_{r,s}$, máme vzorec (??) d
zán.

Uvažujme $t \neq r$ a nahraďme t-tý řádek v matici **A** řádkem r-tým. N
matici označme **C**. Má dva stejné řádky, takže je $\det \mathbf{C} = 0$. Rozvoj to
determinantu podle t-tého řádku odpovídá vzorci (??).

[rozvojsloupce] Vzhledem k platnosti věty ?? platí analogická věta o ro
determinantu podle s-tého sloupce. Zkuste si ji zformulovat jako cvičení.

[doplnek] Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$. *Doplněk matice* ***A*** *v pozici* (i, j) je číslo
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 ma
která vznikne z matice **A** vynecháním i-tého řádku a j-tého sloupce.

[rozvojdoplnku] Větu ?? lze při použití definice ?? a poznámky ?? př
mulovat. Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$ je čtvercová matice a $D_{i,j}$ jsou její doplňky. N
$r, s, t \in \{1, 2, \ldots, n\}$, $r \neq t$, $s \neq t$. Pak platí

$$\det \mathbf{A} = a_{r,1}\,D_{r,1} + a_{r,2}\,D_{r,2} + \cdots + a_{r,n}\,D_{r,n}, \quad 0 = a_{r,1}\,D_{t,1} + a_{r,2}\,D_{t,2} +$$
$$\det \mathbf{A} = a_{1,s}\,D_{1,s} + a_{2,s}\,D_{2,s} + \cdots + a_{n,s}\,D_{n,s}, \quad 0 = a_{1,s}\,D_{1,t} + a_{2,s}\,D_{2,t} +$$

Uvažujme matici **A** z příkladu ?? Provedeme rozvoj determinantu **A** p

Vidíme, že jsme si při výpočtu moc nepomohli. Rozvoj determinantu p
řádku nebo sloupce matice typu (n, n) obecně vede na n determinantů ma
které mají o jediný řádek a sloupec méně. To není žádná výhra.

Kdybychom opakovaně prováděli rozvoj vzniklých determinantů podle
nebo sloupce, mohli bychom dojít až k maticím typu (1,1), u kterých je deter
nant přímo roven hodnotě prvku dané matice. Programátory může napadn
že lze tedy větu o rozvoji determinantu využít při implementaci výpočtu de
minantu rekurzivním algoritmem. Ovšem pozor! Tento algoritmus potřeb
zcela stejné množství operací, jako při výpočtu determinantu přímo z defin
Jak už jsme si uváděli, při matici typu $(50, 50)$ se jedná zhruba o 10^{64} oper
Prakticky to znamená, že bychom se pravděpodobně výsledku nedočkali za
lou dobu předpokládané existence naší sluneční soustavy a kdo ví, jestli b
dříve nezhroutil vesmír.

Můžete namítnout, k čemu že je metoda rozvoje determinantu dob
Pokud se v nějakém řádku nebo sloupci matice vyskytuje mnoho nul, můž
zmenšit velikost matic, ze kterých počítáme determinant. Je-li na řádku n
sloupci jediný nenulový prvek, dostáváme jedinou matici o jeden řádek a slou
menší. V příkladu ?? jsme mohli například před provedením kroku (2) pro
rozvoj determinantu podle prvního sloupce a dále pracovat jen s maticí t
$(3, 3)$. Před krokem (4) jsme mohli znovu provést rozvoj determinantu p
prvního sloupce:

$$\begin{vmatrix} 1 & 2 & 4 & -1 \\ 2 & 1 & 2 & 2 \\ 1 & 3 & 1 & 2 \\ 2 & 1 & 2 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 4 & -1 \\ 0 & -3 & -6 & 4 \\ 0 & 1 & -3 & 3 \\ 0 & -3 & -6 & 3 \end{vmatrix} = 1 \cdot \begin{vmatrix} -3 & -6 & 4 \\ 1 & -3 & 3 \\ -3 & -6 & 3 \end{vmatrix} = - \begin{vmatrix} 1 \\ -3 \\ -3 \end{vmatrix}$$

$$= - \begin{vmatrix} 1 & -3 & 3 \\ 0 & -15 & 13 \\ 0 & -15 & 12 \end{vmatrix} = -1 \cdot \begin{vmatrix} -15 & 13 \\ -15 & 12 \end{vmatrix} = 15 \cdot 12 - 15 \cdot 13 = -15.$$

Důkaz (pro hloubavé čtenáře). Uvědomíme si, že lze matici $\mathbf{A}$ převést p
řádkovými úpravami na matici $\mathbf{A}'$, která je tvaru (??). Navíc můžeme prov
pouze takové úpravy, které nemění determinant: přičítání násobku jiného ř
k řádku podle (V5) věty ?? nemění determinant a pokud potřebujeme proh
řádky, pak okamžitě pronásobíme jeden z nich konstantou -1. Tyto ope
skutečně stačí na převedení matice na tvar (??), a přitom máme zaručen
$\det \mathbf{A} = \det \mathbf{A}'$. Podle věty ?? existuje čtvercová matice $\mathbf{P}$, pro kterou pla

$$\mathbf{A}' = \mathbf{P} \cdot \mathbf{A}.$$

Dále převedeme matici $\mathbf{B}$ na matici $\mathbf{B}'$ tvaru (??) pouze sloupcovými úpra
takovými, které nemění determinant. Máme tedy $\det \mathbf{B} = \det \mathbf{B}'$ a navíc p
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 t
že obě matice $\mathbf{A}'$ i $\mathbf{B}'$ jsou tvaru (??). Matice $\mathbf{A}' \cdot \mathbf{B}'$ je také tvaru
a pro její diagonální prvky $g_{i,i}$ platí, že $g_{i,i} = a'_{i,i} \, b'_{i,i}$. Protože se dete
nanty matic tvaru (??) počítají jako součin prvků na diagonále, máme skut
$\det \mathbf{A}' \, \det \mathbf{B}' = \det(\mathbf{A}' \cdot \mathbf{B}')$.

Na matici $\mathbf{A} \cdot \mathbf{B}$ provedeme stejné řádkové a sloupcové úpravy, jako j
provedli na matice $\mathbf{A}$ resp. $\mathbf{B}$. Dostaneme matici $\mathbf{A}' \cdot \mathbf{B}'$, protože

$$\mathbf{P} \cdot (\mathbf{A} \cdot \mathbf{B}) \cdot \mathbf{Q} = (\mathbf{P} \cdot \mathbf{A}) \cdot (\mathbf{B} \cdot \mathbf{Q}) = \mathbf{A}' \cdot \mathbf{B}'.$$

Důkaz. Podle věty ?? je $\det \mathbf{A} = \det \mathbf{L} \cdot \det \mathbf{U}$. Protože $\det \mathbf{L} = 1$ (ma
diagonále pouze jedničky), je $\det \mathbf{A} = \det \mathbf{U}$ což je podle příkladu ?? so
diagonálních prvků matice $\mathbf{U}$.

[detA-1] 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 $\det \mathbf{A} \cdot \det \mathbf{A}^{-}$
$\det \mathbf{E} = 1$. Vydělením obou stran rovnice číslem $\det \mathbf{A}$ (které je podle vět
nenulové) dostáváme dokazovaný vzorec.

[A-1D] 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 vz
nedělíme nulou. Musíme ověřit, že pro matici $\mathbf{A}^{-1}$ vypočítanou z uveden
vzorce, platí $\mathbf{A} \cdot \mathbf{A}^{-1} = \mathbf{E}$. Je-li $\mathbf{D} = (D_{i,j})$, pak samozřejme je $\mathbf{D}^T = (D$
Podle definice součinu matic ?? vypočítáme prvek $e_{i,k}$ matice $\mathbf{A} \cdot \mathbf{A}^{-1}$:

$$e_{i,k} = \sum_{j=1}^{n} a_{i,j} \, \frac{1}{\det \mathbf{A}} \, D_{k,j} = \frac{1}{\det \mathbf{A}} \big(a_{i,1} D_{k,1} + a_{i,2} D_{k,2} + \cdots + a_{i,n} D_{k,n} \big) = \Bigg\{$$

Zde jsme využili větu o rozvoji determinantu podle i-tého řádku, viz poznám
Zjišťujeme, že prvky $e_{i,k}$ jsou skutečně prvky jednotkové matice ??. Rov
$\mathbf{A}^{-1} \cdot \mathbf{A} = \mathbf{E}$ bychom dokazovali podobně. Použili bychom větu o rozvoji i-
sloupce namísto řádku.

[imatice-dop] Věta ?? kromě teoretických důsledků, které uvidíme poz

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 de
počítají, protože obsahují determinanty matic typu $(1,1)$:

$$\mathbf{D} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}, \qquad \mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}}\, \mathbf{D}^T = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

[pr-imatice-dop] Najdeme inverzní matici ke stejné matici, jako v
kladu ??, 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 nán
trochu práce.

$$\mathbf{D} = \begin{pmatrix} +\begin{vmatrix} 0 & 1 \\ 2 & 1 \end{vmatrix} & -\begin{vmatrix} -1 & 1 \\ 2 & 1 \end{vmatrix} & +\begin{vmatrix} -1 & 0 \\ 2 & 2 \end{vmatrix} \\ -\begin{vmatrix} 2 & 3 \\ 2 & 1 \end{vmatrix} & +\begin{vmatrix} 1 & 3 \\ 2 & 1 \end{vmatrix} & -\begin{vmatrix} 1 & 2 \\ 2 & 2 \end{vmatrix} \\ +\begin{vmatrix} 2 & 3 \\ 0 & 1 \end{vmatrix} & -\begin{vmatrix} 1 & 3 \\ -1 & 1 \end{vmatrix} & +\begin{vmatrix} 1 & 2 \\ -1 & 0 \end{vmatrix} \end{pmatrix} = \begin{pmatrix} -2 & 3 & -2 \\ 4 & -5 & 2 \\ 2 & -4 & 2 \end{pmatrix},$$

$$\det \mathbf{A} = -2, \qquad \mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}}\, \mathbf{B}^T = -\frac{1}{2} \begin{pmatrix} -2 & 4 & 2 \\ 3 & -5 & -4 \\ \ldots \end{pmatrix}.$$

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 $\det \mathbf{A}_1 \det \mathbf{A}_4 - \det \mathbf{A}$
$0 - 0 = 0$.

Že uvedený blokový vzorec neplatí, nás může napadnout i z počtu souč
které obsahuje definice determinantu. Determinant matice z $\mathbf{R}^{2n,2n}$ obsa
$(2n)!$ součinů, zatímco blokový vzorec obsahuje jen $2(n!)^2$ součinů. To je z
jiné číslo.

[detdvabloky] Matici $\mathbf{A} \in \mathbf{R}^{n,n}$ rozdělme na bloky tak, že $\mathbf{A}_1$ a $\mathbf{A}_4$
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 řá
vými úpravami Gaussovy eliminační metody blok $\mathbf{A}_1$ na schodovitou ma
Dá se to navíc provést tak, že matice $\mathbf{A}$ se změní v matici $\mathbf{A}' = (a'_{i,j})$ se stej
determinantem a pracujeme jen s prvními m řádky matice $\mathbf{A}$. Podle ?? p
$\det \mathbf{A}_1 = a'_{1,1} \cdot a'_{2,2} \cdots a'_{m,m}$. Dokazovaný vzorec je pak výsledkem opakovan
rozvoje determinantu matice $\mathbf{A}'$ podle prvního sloupce, podle druhého slou
atd. až podle m-tého sloupce.

[detbloku] 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}

Důkaz. Analogicky, jako v příkladu ??. Má-li se to provést pořádně, je poti
použít indukci podle k, přičemž argumenty v příkladu ?? poslouží pro indu
krok.

Determinant čtvercové matice je definován jako součet součinů prvků
tice opatřených jistým znaménkem. Podrobněji viz ??.

Determinant je možné vypočítat i rekurzivním algoritmem pomocí vě
rozvoji determinantu podle řádku či sloupce /??, ??/.

Determinant se nezmění, pokud modifikujeme matici tak, že k jedn
řádku/sloupci přičítáme α-násobek řádku/sloupce jiného. Násobíme-li je
řádek/sloupec nenulovou konstantou, stejnou konstantou je násoben de
minant. Prohodíme-li dva řádky/sloupce, determinant změní znaménko /
Díky těmto vlastnostem můžeme hlídat změny v determinantu při všech kro
Gaussovy eliminační metody. Ta nám umožní převést matici na schodovi
tedy horní trojúhelníkovou matici. Ta má determinant roven součinu prvku
diagonále /??/. To nám dává metodu na počítání determinantů pomocí G
sovy eliminační metody. Tato metoda je výpočtově výrazně méně náročná
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 /??/ transpon
nou a násobenou převrácenou hodnotou determinantu /??/. To není efekt
metoda, ale má své teoretické důsledky, například při důkazu Cramerova
vidla /??/ z následující kapitoly.

9. Soustavy lineárních rovnic

[dsoustava] 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 $\boldsymbol{b} = (b_1, b_2, \ldots, b_m)^T \in \mathbf{R}$ je sloupcový vektor reálných čísel. Pak maticovou rovnost

$$\mathbf{A} \cdot \boldsymbol{x} = \boldsymbol{b}$$

navývíme *soustavou m lineárních rovnic o n neznámých*. Matici $\mathbf{A}$ nazýv *maticí soustavy* a vektor $\boldsymbol{b} = (b_1, \ldots, b_m)^T$ nazýváme *vektorem pravých st* Připíšeme-li k matici soustavy do dalšího sloupce vektor $\boldsymbol{b}$ oddělený (pouze přehlednost) svislou čarou, dostáváme matici $(\mathbf{A}|\boldsymbol{b}) \in \mathbf{R}^{m,n+1}$, kterou n váme *rozšířenou maticí soustavy*.

[dreseni] *Řešením soustavy* $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ je takový vektor $\boldsymbol{v} = (\alpha_1, \alpha_2, \ldots, \alpha$ $\mathbf{R}^{n,1}$, pro který platí: dosadíme-li hodnoty α_i za symboly x_i, pak je spl požadovaná maticová rovnost, tj.

$$\mathbf{A} \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} .(resenisoustavy)$$

Řešit soustavu $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ znamená nalézt všechna její řešení, tj. nalézt podm žinu $\mathbf{R}^{n,1}$ všech řešení této soustavy.

[Rn=Rn1] Ačkoli přesně řečeno je množina řešení podmnožinou slou vých vektorů $\mathbf{R}^{n,1}$, často složky těchto řešení nakonec píšeme do řádků izomorfismus zmíněný v poznámce ??). Mluvíme tedy o množině řešení ja podmnožině $\mathbf{R}^n$. Jinými slovy, nedojde-li k nedorozumění, zapisujeme jed livá řešení soustavy $\boldsymbol{v} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ jako prvky z $\mathbf{R}^n$.

* [frobeni] Soustava $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ má řešení právě tehdy, když hod $\mathbf{A}$ = hod(
tj. když hodnost matice soustavy se rovná hodnosti rozšířené matice soust

Protože platí věta ??, je Frobeniova věta dokázána.

V úvodní kapitole o Gaussově eliminační metodě jsme vlastně nevědo vyslovili Frobeniovu větu. V této kapitole jsme si říkali, jak poznáme, že stava má řešení. Mluvili jsme tam o tom, že soustava nemá řešení právě te když poslední řádek rozšířené matice soustavy po přímém chodu eliminac 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 e tence takového řádku je ekvivalentní s tím, že rozšířená matice soustavy m jedničku větší hodnost, než matice soustavy. Uvědomíme si ještě, že hod rozšířené matice soustavy může být buď o jedničku větší nebo přímo ro hodnosti matice soustavy. Žádná jiná možnost pro hodnosti těchto matic xistuje.

[eqsoust] Nechť $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ je soustava m lineárních rovnic o n neznámý $\mathbf{C}\,\boldsymbol{x} = \boldsymbol{d}$ je soustava k lineárních rovnic o stejném počtu n neznámých. Říká že tyto soustavy jsou *ekvivalentní*, pokud obě soustavy mají stejné mno řešení.

Gaussova eliminační metoda řešení soustav lineárních rovnic popsaná v kapitole spočívá v převedení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ na soustavu $\mathbf{C}\,\boldsymbol{x} = \boldsymbol{d}$, kter s původní soustavou rovnic ekvivalentní. Přitom řešení soustavy $\mathbf{C}\,\boldsymbol{x} = \boldsymbol{d}$ nalézt snadněji, protože $\mathbf{C}$ je schodovitá matice (srovnejte větu ??). Tuto tečnost zaznamenáme do následující věty.

[exeqsoust] Ke každé soustavě $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ lze nalézt ekvivalentní soust $\mathbf{C}\,\boldsymbol{x} = \boldsymbol{d}$, 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 při $\mathbf{C}$ je schodovitá matice. Protože operace „$\sim$“ zde označuje konečně m elementárních kroků Gaussovy eliminační metody, a protože jsme si řek

* [homolinprst] Množina všech řešení homogenní soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$ neznámými tvoří lineární podprostor lineárního prostoru $\mathbf{R}^n$.

Důkaz. Věta by správně měla znít: množina řešení homogenní soustavy t lineární podprostor lineárního prostoru $\mathbf{R}^{n,1}$, ovšem v souladu s poznámko nebudeme rozlišovat mezi $\mathbf{R}^{n,1}$ a $\mathbf{R}^n$.

Především množina řešení homogenní soustavy je neprázdná, protože lový 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 $\boldsymbol{v} \in$ řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$, pak též $\boldsymbol{u} + \boldsymbol{v}$ je řešením stejné soustavy. (2) $\boldsymbol{u} \in \mathbf{R}^{n,1}$ řešením soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$ a $\alpha \in \mathbf{R}$, pak též $\alpha\,\boldsymbol{u}$ je řešením st soustavy.

Protože $\boldsymbol{u}$ a $\boldsymbol{v}$ jsou řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$, platí: $\mathbf{A}\,\boldsymbol{u} = \boldsymbol{o}$ a $\mathbf{A}\,\boldsymbol{v}$ = Máme dokázat, že pak také $\mathbf{A}\,(\boldsymbol{u} + \boldsymbol{v}) = \boldsymbol{o}$ a $\mathbf{A}\,(\alpha\,\boldsymbol{u}) = \boldsymbol{o}$. Podle věty ?? j

$$\mathbf{A}\,(\boldsymbol{u} + \boldsymbol{v}) = \mathbf{A}\,\boldsymbol{u} + \mathbf{A}\,\boldsymbol{v} = \boldsymbol{o} + \boldsymbol{o} = \boldsymbol{o},$$
$$\mathbf{A}\,(\alpha\,\boldsymbol{u}) = \alpha\,\mathbf{A}\,\boldsymbol{u} = \alpha\,\boldsymbol{o} = \boldsymbol{o}.$$

[homoprikl] Najdeme množinu všech řešení homogenní soustavy lineár rovnic se šesti neznámými:

$$\begin{array}{rcrcrcrcrcrcl} x_1 &+& x_2 &+& 2x_3 &+& 3x_4 &+& 3x_5 &+& 3x_6 &=& 0 \\ x_1 &+& x_2 &+& x_3 &+& 3x_4 &+& x_5 &+& x_6 &=& 0 \\ 2x_1 &+& 2x_2 &+& 2x_3 &+& 6x_4 &+& 2x_5 &+& 8x_6 &=& 0 \end{array}$$

Eliminujeme matici soustavy (vektor pravých stran je nulový, takže je zbyte jej psát).

z předposlední rovnice máme $x_3 = -2v$ a konečně z první rovnice dostáv
$x_1 = -t + 4v - 3u - 3v = -t + v - 3u$. Výsledek sumarizujeme takto:

$$(x_1, x_2, x_3, x_4, x_5, x_6) = (-t + v - 3u,\ t,\ -2v,\ u,\ v,\ 0) =$$
$$= t\,(-1, 1, 0, 0, 0, 0) + u\,(-3, 0, 0, 1, 0, 0) + v\,(1, 0, -2,$$

Z tohoto zápisu vyplývá, že množina všech řešení dané homogenní soust
je množinou všech lineárních kombinací uvedených tří vektorů, což můž
zapsat pomocí lineárního obalu takto:

$$M_0 = \big\langle (-1, 1, 0, 0, 0, 0), (-3, 0, 0, 1, 0, 0), (1, 0, -2, 0, 1, 0) \big\rangle.$$

Protože uvedené tři vektory z výsledku příkladu ?? jsou lineárně nezáv
tvoří jednu z možných bází prostoru M_0. To se nestalo náhodou, ale plat
vždy, jak ukazuje následující věta.

[homoveta] Nechť $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$ je homogenní soustava lineárních rovnic o n
známých, $k = n -$hod $\mathbf{A}$. Pak existuje k lineárně nezávislých vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2,$
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 v
řešení M_0.

Důkaz. Vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ najdeme analogicky, jako jsme to udělali v
kladu ??. Algoritmus ?? zaručuje, že počet rovnic soustavy po eliminaci je ro
hod $\mathbf{A}$ a je roven počtu neznámých, které můžeme z rovnic vypočítat. Ostat
$k = n -$ hod $\mathbf{A}$ neznámých $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$ může nabývat libovolných hod
a zaveďme pro ně parametry $x_{i_1} = p_1, x_{i_2} = p_2, \ldots, x_{i_k} = p_k$. Všechna ře
získáme například dosazovací metodou použitou na rovnice po eliminaci
čínáme poslední rovnicí a končíme první). Z tohoto řešení můžeme vytkn

Zbývá dokázat, že vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ jsou lineárně nezávislé. Ozna $\boldsymbol{u}'_1 \in \mathbf{R}^k$, $\boldsymbol{u}'_2 \in \mathbf{R}^k, \ldots,$ $\boldsymbol{u}'_k \in \mathbf{R}^k$ ty části vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$, které obsa jen složky $i_1, i_2, \ldots, i_k$. Protože platí rovnost (??) a také platí označení x $p_1, x_{i_2} = p_2, \ldots, x_{i_k} = p_k$, 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 nezávi vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$, 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 ře homogenní soustavy, plyne přímo z definice báze ??.

* [dimhomo] Nechť M_0 je lineární prostor všech řešení homogenní soust 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 ??.

Nechť n je počet neznámých homogenní soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$. Pak z vět plyne tento důsledek:

$$\begin{array}{ll} \operatorname{hod} \mathbf{A} = n & \text{pak soustava má jen nulové řešení,} \\ \operatorname{hod} \mathbf{A} < n & \text{pak soustava má nekonečně mnoho řešení.} \end{array}$$

[partikul] Nechť $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ je nehomogenní soustava lineárních rovnic neznámých a $\boldsymbol{v} \in \mathbf{R}^n$ je nějaké jedno její řešení. Takovému řešení $\boldsymbol{v}$ řík *partikulární řešení* nehomogenní soustavy.

Pokud zaměníme sloupcový vektor $\boldsymbol{b}$ za nulový vektor stejného typu, do váme homogenní soustavu $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$, kterou nazýváme *přidruženou homog soustavou* k soustavě $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$.

[nehomoprst] (1) Nechť $\boldsymbol{v}$ je partikulární řešení nehomogenní soust $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ a $\boldsymbol{u}$ je libovolné řešení přidružené homogenní soustavy $\mathbf{A}\,\boldsymbol{x} =$

(2) Podle předpokladu platí $\mathbf{A}\,\boldsymbol{v} = \boldsymbol{b}$, $\mathbf{A}\,\boldsymbol{w} = \boldsymbol{b}$. Pro rozdíl $\boldsymbol{v} - \boldsymbol{w}$ pak plat

$$\mathbf{A}\,(\boldsymbol{v} - \boldsymbol{w}) = \mathbf{A}\,\boldsymbol{v} - \mathbf{A}\,\boldsymbol{w} = \boldsymbol{b} - \boldsymbol{b} = \boldsymbol{o}.$$

* [partikul+obal] Nechť $\boldsymbol{v}$ je partikulární řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ a M lineární prostor všech řešení přidružené homogenní soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$. Pak množinu M všech řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ platí

$$M = \big\{\boldsymbol{v} + \boldsymbol{u};\ \ \boldsymbol{u} \in M_0\big\}.$$

Důkaz. Z vlastnosti (1) věty ?? plyne, že $\{\boldsymbol{v} + \boldsymbol{u};\ \ \boldsymbol{u} \in M_0\} \subseteq M$. S 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 obráce inkluze.

[v+M0] Množinu všech řešení nehomogenní soustavy lineárních rovnic pisujeme většinou zjednodušeně jako součet partikulárního řešení a lineár prostoru všech řešení přidružené homogenní soustavy takto:

$$M = \boldsymbol{v} + M_0 = \boldsymbol{v} + \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle.(nehomoreseni)$$

Řešit nehomogenní soustavu tedy znamená najít partikulární řešení $\boldsymbol{v}$ a dále jít k lineárně nezávislých řešení přidružené homogenní soustavy $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots$ (k je rovno počtu neznámých mínus hodnost matice soustavy). Výslede obvyklé psát ve tvaru (??).

[nehomoruc] Najdeme množinu všech řešení soustavy lineárních rovni šesti neznámými:

$$\begin{aligned}
x_1 + x_2 + 2x_3 + 3x_4 + 3x_5 + 3x_6 &= 1\\
x_1 + x_2 + x_3 + 3x_4 + x_5 + x_6 &= -1
\end{aligned}$$

Z poslední rovnice budeme počítat x_6, z předposlední rovnice x_3 a z p
rovnice x_1. Hodnoty neznámých x_2, x_4, x_5 mohou být libovolné. Zaveďme
ně parametry $x_2 = t$, $x_4 = u$, $x_5 = v$.

Z poslední rovnice máme $x_6 = 2$, z předposlední rovnice $x_3 = 2-2v-2$
$-2 - 2v$ a konečně z první rovnice dostáváme $x_1 = 1 - t - 2(-2 - 2v) - 3$
$3v - 3 \cdot 2 = -1 - t + v - 3u$. Výsledek sumarizujeme takto:

$$(x_1, x_2, x_3, x_4, x_5, x_6) = (-1 - t + v - 3u, t, -2 - 2v, u, v, 2) =$$
$$= (-1, 0, -2, 0, 0, 2) + t\,(-1, 1, 0, 0, 0, 0) + u\,(-3, 0, 0$$

Z tohoto zápisu vyplývá, že množina všech řešení dané nehomogenní soust
je rovna

$$M = (-1, 0, -2, 0, 0, 2) + \big\langle(-1, 1, 0, 0, 0, 0), (-3, 0, 0, 1, 0, 0), (1, 0, -2, 0, 1,$$

Vektor $(-1, 0, -2, 0, 0, 2)$ je partikulárním řešením dané nehomogenní soust
a vektory $(-1, 1, 0, 0, 0, 0)$, $(-3, 0, 0, 1, 0, 0)$, $(1, 0, -2, 0, 1, 0)$ tvoří bázi pros
řešení přidružené homogenní soustavy.

Ve výše uvedeném příkladě jsem spočítali partikulární řešení i bázi n
žiny řešení přidružené homogenní soustavy v jediném postupu. Často ale
kovéto lineární úlohy řešíme ve dvou krocích. Nejprve najdeme bázi řešení
družené homogení soustavy (to jsme provedli v příkladu ??) a poté je t
„uhodnout“ jedno řešení dané nehomogení soustavy. Takové řešení prohlás
za partikulární řešení. Nakonec zapíšeme výsledek v souladu s poznámko
ve formě „partikulární řešení plus lineární obal báze množiny řešení přidru
homogenní soustavy“.

Partikulární řešení můžeme najít po přímém chodu eliminační met
když rozhodneme, které proměné budeme pomocí rovnic počítat. Těm ostat
proměným můžeme přidělit jakákoli čísla, třeba nuly. Po dosazení těchto
vzniká soustava, která má stejně rovnic jako neznámých a má regulární ma
tedy má jediné řešení. Toto řešení obsahuje hodnoty hledaných proměnný

Nyní můžeme použít zpětný chod Gaussovy eliminační metody nebo počítat
sazovací metodou od poslední rovnice k první. Dostáváme řešení $x_1 = -1,$
$-2, x_6 = 2$, takže partikulárním řešením je $(-1, 0, -2, 0, 0, 2)$.

Při strojovém hledání řešení rozsáhlých soustav většinou jde o to n
jedno partikulární řešení a bázi prostoru řešení přidružené homogenní soust
Přitom není nutné programovat symbolické výpočty, jako je například vytýk
parametrů podle rovnosti (??). V následujícím textu ukážeme, že stačí vy
Gaussovu eliminační metodu.

K nalezení báze přidružené homogenní soustavy můžeme použít násled
větu ?? a k nalezení partikulírního řešení využijeme větu ??.

[genbasehomo] Nechť homogenní soustava lineárních rovnic $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$
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.
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
stavy je n, takže matice soustavy $\mathbf{A}$ je typu (m, n). Počet sloupců n této ma
se skládá z m sloupců (matice $\mathbf{E}$) a k sloupců (matice $\mathbf{C}$). Je tedy $n = m$
Dimenze prostoru řešení je podle věty ?? rovna počtu neznámých minus ho
což je $n - m = k$. To sedí. Skutečně matice $\mathbf{B} = (-\mathbf{C}^T|\mathbf{E}')$ má k řádků a

Tato věta nám umožňuje rovnou napsat bázi řešení homogenní soust pokud je matice soustavy v uvedeném tvaru. Dokonce, pokud matice soust není v uvedeném tvaru, je někdy možné jí eliminací do tohoto tvaru přev tj. ekvivalentní soustava může mít tento tvar. Pokud ani ekvivalentní sous nemá tento tvar, dá se prohozením pořadí neznámých dospět k požadovan tvaru matice soustavy. V takovém případě je ovšem nutné před zapsáním prostoru řešení prohodit sloupce matice $\mathbf{B} = (-\mathbf{C}^T|\mathbf{E}')$ zpět. Místo dlouh vysvětlování ukážeme použití věty na našem příkladu ??.

[homostroj] Najdeme bázi prostoru řešení soustavy z příkladu ??. El nujeme matici soustavy:

$$\begin{pmatrix} 1 & 1 & 2 & 3 & 3 & 3 \\ 1 & 1 & 1 & 3 & 1 & 1 \\ 2 & 2 & 2 & 6 & 2 & 8 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 3 & 3 & 3 \\ 0 & 0 & -1 & 0 & -2 & -2 \\ 0 & 0 & -2 & 0 & -4 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 3 & 3 & 3 \\ 0 & 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Eliminujeme dále zpětným chodem, abychom ve sloupcích 1, 3 a 6 dostali notkové 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 (měn 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 tako maticí můžeme podle této věty zapsat do matice, kde každý řádek obsa jeden vektor báze:

$$\begin{pmatrix} -3 & 0 & 0 & 1 & 0 & 0 \\ 1 & -2 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

[genpartikul] Nechť soustava lineárních rovnic $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ má matici soust 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. partikulárním řešením soustavy je vektor $\boldsymbol{v} = (\boldsymbol{b}^T, \boldsymbol{o})$, kde $\boldsymbol{o} \in \mathbf{R}^k$ je nu vektor.

Důkaz. Stačí dosadit:

$$\mathbf{A} \cdot \begin{pmatrix} \boldsymbol{b} \\ \boldsymbol{o} \end{pmatrix} = (\mathbf{E}\,|\,\mathbf{C}) \begin{pmatrix} \boldsymbol{b} \\ \boldsymbol{o} \end{pmatrix} = \mathbf{E}\boldsymbol{b} + \mathbf{C}\boldsymbol{o} = \boldsymbol{b}.$$

[pstroj] V tomto příkladě si ukážeme „strojové“ řešení soustav lineár rovnic s využitím vět ?? a ??. K řešení nepotřebujeme nic jiného než d namazaný stroj zvládající přímý a zpětný chod Gaussovy eliminační meto

Najdeme množinu řešení soustavy lineárních rovnic s rozšířenou mati

$$\left(\begin{array}{rrrrr|r} 1 & 1 & -1 & 11 & 1 & 3 \\ 1 & 2 & 2 & 8 & 2 & 5 \\ 2 & 5 & 7 & 17 & 6 & 18 \\ 3 & 6 & 6 & 28 & 7 & 21 \end{array}\right)$$

Pomocí přímého chodu eliminační metody matici převedeme na schod tou matici. Po prohození třetího sloupce s posledním pak dostáváme matic které můžeme použít zpětný chod Gaussovy eliminační metody tak, že v le bloku dostaneme jednotkovou matici. Nad maticí jsme si poznamenali změ pořadí proměných.

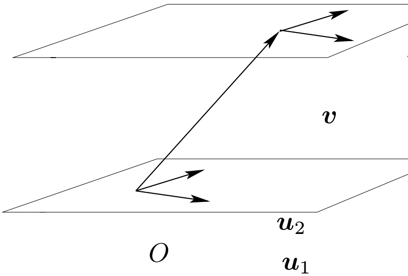
$$\left(\begin{array}{rrrrr|r} 1 & 1 & -1 & 11 & 1 & 3 \\ 1 & 2 & 2 & 8 & 2 & 5 \\ 2 & 5 & 7 & 17 & 6 & 18 \end{array}\right) \sim \begin{array}{c} \begin{array}{ccccc} x_1 & x_2 & x_3 & x_4 & x_5 \end{array} \\ \left(\begin{array}{rrrrr|r} 1 & 1 & -1 & 11 & 1 & 3 \\ 0 & 1 & 3 & -3 & 1 & 2 \end{array}\right) \end{array} \leftrightarrow \begin{array}{c} \begin{array}{ccccc} x_1 & x_2 & x_5 & x_4 & x_3 \end{array} \\ \left(\begin{array}{rrrrr|r} 1 & 1 & 1 & 11 & -1 & 3 \\ 0 & 1 & 1 & -3 & 3 & 2 \end{array}\right) \end{array}$$

a podle věty ?? je partikulární řešení ve tvaru $(1, -4, 6, 0, 0)$. Po zpětném př
zení sloupců tak, abychom popsali výsledek pro neznámé v pořadí $(x_1, x_2, x_3$
dostáváme řešení:

$$(1, -4, 0, 0, 6) + \langle (-14, 7, 0, 1, -4),\ (4, -3, 1, 0, 0) \rangle,$$

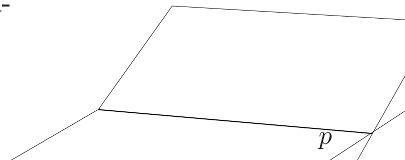
které jsme zapsali jako součet partikulárního řešení a lineárního obalu b
množiny řešení přidružené homogenní soustavy, tedy v souladu s poznámkou

[geomnadroviny] 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
řadnicemi $(0, 0, 0)$. V případě, že soutava má nenulovou pravou stranu,
množinou řešení je rovina, která neprochází počátkem. Je to rovina ϱ rov
běžná s množinou řešení přidružené homogenní soustavy ϱ' a prochází bod
který je dán jako partikulární řešení $\boldsymbol{v}$. Viz obrázek.

[pruniknadrovin] Představme si soustavu dvou lineárně nezávislých lineárních rovnic o třech neznámých. Množinu řešení interpretujme jako body v prostoru stejně jako v předchozí po-



Tři lineárně nezávislé rovnice o třech neznámých mají jednobodové řeš které je průnikem tří rovin, kde každá rovina je množinou řešení jedné rovn

Nemá-li soustava tří rovnic o třech neznámých řešení, pak jednotlivé nice mají jako své množiny řešení roviny, které nemají společný průnik. U domíme si, jakým způsobem se to může stát: buď jsou dvě roviny rovnobě a nikoli totožné, nebo mají roviny jako průnik přímky, které jsou rovnoběž

* [nadrovina] Má-li soustava lineárních rovnic n neznámých, pak množ řešení je podmnožina $\mathbf{R}^n$. Představme si, že nyní $n > 3$. S trochou fantaz možné si i tyto podmnožiny představit geometricky jako *zobecněné roviny*

Pojem *zobecněná rovina* se používá pro analogický geometrický útvar je rovina nebo přímka v geometrickém prostoru, ale může mít libovolnou (tř větší) dimenzi. Zobecněná rovina nemusí na rozdíl od lineárního podpros procházet počátkem. Pokud ji ale posuneme do počátku, tvoří podpros Mluvíme-li tedy o *dimenzi zobecněné roviny*, máme na mysli dimenzi lin ního podprostoru, který vznikne posunutím zkoumané zobecněné roviny aby procházela počátkem.

Množina řešení jedné rovnice ze soustavy je zobecněná rovina, která dimenzi $n-1$. Množina řešení celé soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ je průnikem těchto zo něných rovin a je to zase zobecněná rovina ϱ, která má podle věty ?? dim $n - \operatorname{hod} \mathbf{A}$. Množina řešení přidružené homogenní soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$ je zo něná rovina ϱ' taková, že prochází počátkem a $\varrho = \boldsymbol{v} + \varrho'$, kde $\boldsymbol{v}$ je partikul řešení. Tedy ϱ vzniká z ϱ' posunutím o $\boldsymbol{v}$. Nebo obráceně, ϱ' vzniká posunu ϱ o vektor $-\boldsymbol{v}$.

Obrázky u poznámek ?? a ?? lze využít jako ilustraci pro množiny ře libovolné soustavy lineárních rovnic. První obrázek říká, že zobecněná rov která je množinou řešení nehomogenní soustavy lineárních rovnic, je posun z počátku o partikulární řešení. Druhý obrázek říká, že množina řešení je becněná rovina, která je průnikem nadrovin, které jsou řešeními jednotliv můžeme přepsat takto:

$$\mathbf{A} \cdot \mathbf{x} \; = \; (\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n) \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \; x_1 \mathbf{A}_1 + x_2 \mathbf{A}_2 + \cdots + x_n \mathbf{A}_n \; =$$

takže řešení obsahuje koeficienty takové lineární kombinace sloupců, kter
rovna vektoru pravých stran $\boldsymbol{b}$.

[popis-reseni] Již v úvodní kapitole o Gaussově eliminační metodě j
zmínili, že množinu řešení soustavy lineárních rovnic neumíme popsat je
značným způsobem. Výjimkou je pouze případ, kdy má soustava jediné řeš
Víme totiž, že každý netriviální lineární podprostor má nekonečně mnoho
a má-li soustava více řešení, pak i partikulární řešení může každý řešitel za
jiné.

K různým zápisům téže množiny řešení můžeme dospět při výpočtu t
tak, že volíme rozdílnou skupinu neznámých, které mohou nabývat libovoln
hodnot. I při stejné skupině těchto neznámých nás nikdo nenutí, abychom
neznámé položili rovny jednonásobku parametru. V modelových řešeních
kladů ze skript se můžeme setkat někdy i s jinak volenými parametry tak,
výsledek vyšel bez použití zlomků pouze s malými celými čísly. Tuto do
nost nebudeme v praktických příkladech (které nejsou modelové) potřebo
takže nás nemusí frustrovat, že nám vycházejí ve výsledcích zlomky. Můž
ovšem v závěru výpočtu každý vektor báze vynásobit společným jmenovate
všech zlomků v jednotlivých složkách a znovu dostáváme vektory báze stejn
lineárního prostoru, tentokrát s celočíselnými složkami.

Kvůli nejednoznačnosti popisu řešení soustav lineárních rovnic je užite
vědět, jak poznáme, že dva různé popisy řešení popisují stejnou množinu řeš
To je rozebráno podrobně v následující poznámce.

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 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.

Prověříme, zda množina

$$M_1 = (1, 2, -4, -1, 1, 2) + \big\langle (7, 1, -4, -2, 2, 0), (-8, 3, -2, 2, 1, 0), (2, -2, -6,$$

je rovna množině M z příkladu ??.

Díky tomu, že naše řešení z příkladu ?? obsahuje na pozicích 2, 4 systematicky rozmístěné nuly a jedničky, můžeme okamžitě pohledem do tě pozic psát následující koeficienty lineárních kombinací:

$$\begin{aligned}
(7, 1, -4, -2, 2, 0) &= 1\,(-1, 1, 0, 0, 0, 0) - 2\,(-3, 0, 0, 1, 0, 0) + 2\,(1, 0, -2, 0 \\
(-8, 3, -2, 2, 1, 0) &= 3\,(-1, 1, 0, 0, 0, 0) + 2\,(-3, 0, 0, 1, 0, 0) + 1\,(1, 0, -2, 0 \\
(2, -2, -6, 1, 3, 0) &= -2\,(-1, 1, 0, 0, 0, 0) + 1\,(-3, 0, 0, 1, 0, 0) + 3\,(1, 0, -2, 0 \\
(1, 2, -4, -1, 1, 2) &= (-1, 0, -2, 0, 0, 2) + 2\,(-1, 1, 0, 0, 0, 0) - 1\,(-3, 0, 0, 1, 0
\end{aligned}$$

tory). Zjistíme, že jsou lineárně nezávislé. Pak spočítáme hodnost matice

$$\mathbf{C}^T = \begin{pmatrix} -1 & -3 & 1 & 7 & -8 & 2 & -2 \\ 1 & 0 & 0 & 1 & 3 & -2 & -2 \\ 0 & 0 & -2 & -4 & -2 & -6 & 2 \\ 0 & 1 & 0 & -2 & 2 & 1 & 1 \\ 0 & 0 & 1 & 2 & 1 & 3 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} -1 & -3 & 1 & 7 & -8 & 2 & -2 \\ 0 & -3 & 1 & 8 & -5 & 0 & -4 \\ 0 & 1 & 0 & -2 & 2 & 1 & 1 \\ 0 & 0 & -2 & -4 & -2 & -6 & 2 \\ 0 & 0 & 1 & 2 & 1 & 3 & -1 \end{pmatrix} \sim$$

Je $\operatorname{hod} \mathbf{C} = 3$, takže platí $M = M_1$.

Je-li $\mathbf{A}$ čtvercová matice, pak je výhodné při řešení soustavy $\mathbf{A}\,\boldsymbol{x}$ spočítat $\det \mathbf{A}$.

Pro $\det \mathbf{A} \neq 0$ je $\operatorname{hod} \mathbf{A}$ rovna počtu neznámých, tj. matice $\mathbf{A}$ je regulár soustava má jediné řešení. Množina řešení přidružené homogenní soustavy o huje totiž v tomto případě jediné řešení: nulový vektor. Po vynásobení rovn $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ inverzní maticí $\mathbf{A}^{-1}$ zleva máme okamžitě řešení soustavy $\boldsymbol{x} = \mathbf{A}$ Navíc můžeme použít pro zjištění jednotlivých složek řešení tzv. Cramer pravidlo (viz následující větu).

Pro $\det \mathbf{A} = 0$ je $\operatorname{hod} \mathbf{A}$ menší než počet neznámých. Pokud má tato stava podle Frobeniovy věty ?? řešení, pak po eliminaci a odstranění nulov řádků dostáváme soustavu, která už nemá čtvercovou matici. V tomto příp nezbývá nic jiného, než použít postup pro nalezení všech řešení, který by vyložen dříve.

* [cramer] Nechť $\mathbf{A}$ je regulární čtvercová matice. Pak pro i-tou slo řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ platí

$$\alpha_i = \frac{\det \mathbf{B}_i}{\det \mathbf{A}}\,,$$

Nechť b_i jsou složky sloupce $\boldsymbol{b}$. Podle definice maticového násobení je

$$\alpha_i = \sum_{j=1}^{n} c_{i,j}\, b_j = \sum_{j=1}^{n} \frac{D_{j,i}}{\det \mathbf{A}}\, b_j = \frac{1}{\det \mathbf{A}} \Big(D_{1,i}\, b_1 + D_{2,i}\, b_2 + \cdots + D_{k,i}\, b_k \Big) =$$

V poslední rovnosti jsme využili větu o rozvoji determinantu matice $\mathbf{B}_i$ p
i-tého sloupce, viz poznámku ??.

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:

$$x_1 = \frac{1}{D} \begin{vmatrix} 10 & 2 & 3 \\ 11 & 4 & 5 \\ 12 & 6 & 8 \end{vmatrix}, \quad x_2 = \frac{1}{D} \begin{vmatrix} 1 & 10 & 3 \\ 3 & 11 & 5 \\ 5 & 12 & 8 \end{vmatrix}, \quad x_3 = \frac{1}{D} \begin{vmatrix} 1 & 2 & 10 \\ 3 & 4 & 11 \\ 5 & 6 & 12 \end{vmatrix}, \quad \text{kde}$$

Vypočítáním čtyř determinantů z uvedených matic typu (3,3) dostáváme
sledek

$$x_1 = \frac{18}{-2} = -9, \quad x_2 = \frac{-19}{-2} = \frac{19}{2}, \quad x_3 = \frac{0}{-2} = 0, \quad (x_1, x_2, x_3) = \Big(-9,$$

Cramerovo pravidlo se nejeví pro výpočet řešení soustavy s regulární
ticí příliš účelné. Potřebujeme spočítat $n+1$ determinantů matic typu $(n$
což je pro velká n náročnější, než spočítat inverzní matici eliminační meto
Výhodná může být tato metoda pouze tehdy, když nepotřebujeme znát všec
složky řešení, ale jen některé. Například můžeme mít nějaký fyzikální m

Rozlišíme různé množiny řešení této soustavy podle hodnot reálného param
p.

Determinant matice soustavy je roven $D = p\,(2-p)$, takže pro p
a $p \neq 2$ je matice soustavy regulární a soustava má jediné řešení. Napří
Cramerovým pravidlem zjistíme toto řešení:

$$x = \frac{1}{D}\begin{vmatrix} 1 & p & 1 \\ -1 & 2 & 1 \\ -1 & 1 & p \end{vmatrix} = \frac{p+1}{2-p}, \quad y = \frac{1}{D}\begin{vmatrix} 1 & 1 & 1 \\ 1 & -2 & 0 \\ 0 & -1 & p \end{vmatrix} = \frac{2}{p-2}, \quad z = \frac{1}{D}\begin{vmatrix} 1 \\ 1 \\ 0 \end{vmatrix}$$

Pro $p = 0$ a $p = 2$ musíme řešit soustavu individuálně.

$$p = 0: \quad \left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 1 & 2 & 1 & -1 \\ 0 & 1 & 0 & -1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & -1 \end{array}\right),$$

při $z = t$, vychází $y = -1$, x
tj. $(x, y, z) = (1-t, -1, t) =$
$t(-1, 0, 1)$,
množina řešení: $M = (1, -1,$

$$p = 2: \quad \left(\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ 1 & 2 & 1 & -1 \\ 0 & 1 & 2 & -1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & -1 \end{array}\right),$$

podle Frobeniovy věty soust

[AX=B] Seznámíme se s možnostmi řešení většího množství soustav lin
ních rovnic se stejnou maticí soustavy, ale s různými pravými stranami. M
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 ?? vid
že uvedená soustava soustav je ekvivalentní maticové rovnici

$i \in \{1, 2, \ldots, k\}$, kde $\boldsymbol{v}_i$ je partikulární i-té soustavy a M_0 je množina ře přidružené homogenní soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$. Ta je společná všem soustavám.

Při řešení takových soustav soustav je přirozené před zahájením elimin zapsat všechny sloupce pravých stran vedle sebe a eliminovat společně c matici. To ilustruje následující 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:

$$\left(\begin{array}{cccccc|cccc} 1 & 1 & 2 & 3 & 3 & 3 & 2 & 4 & 3 & 3 \\ 1 & 1 & 1 & 3 & 1 & 1 & 2 & 2 & 1 & 3 \\ 2 & 2 & 2 & 6 & 2 & 8 & 1 & 2 & 3 & 4 \end{array}\right) \sim \left(\begin{array}{cccccc|cccc} 1 & 1 & 2 & 3 & 3 & 3 & 2 & 4 & 3 & 3 \\ 0 & 0 & 1 & 0 & 2 & 2 & 0 & 2 & 2 & 0 \\ 0 & 0 & 2 & 0 & 4 & -2 & 3 & 6 & 3 & 2 \end{array}\right) \sim \left(\begin{array}{cc} 1 & 1 \\ 0 & 0 \\ 0 & 0 \end{array}\right.$$

Přidruženou homogenní soustavu známe už z předchozích příkladů, takže v že její prostor řešení má bázi $\{(-1, 1, 0, 0, 0, 0), (-3, 0, 0, 1, 0, 0), (1, 0, -2, 0,$ Partikulární řešení budeme hledat pro každý sloupec pravých stran zvlášť. P tat budeme poslední, třetí a první složku, v ostatních předpokládáme nuly. sloupec $(2, 0, -3)^T$ máme řešení $(\frac{3}{2}, 0, 1, 0, 0, -\frac{1}{2})$, pro sloupec $(4, 2, -2)^T$ m řešení $(-\frac{1}{3}, 0, \frac{8}{3}, 0, 0, -\frac{1}{3})$, pro sloupec $(3, 2, 1)^T$ máme řešení $(-\frac{5}{6}, 0, \frac{5}{3}, 0,$ a konečně pro sloupec $(3, 0, -2)^T$ máme řešení $(\frac{8}{3}, 0, \frac{2}{3}, 0, 0, -\frac{1}{3})$. Zapíšem tato řešení do sloupců vedle sebe, máme jedno z možných řešení pro hl nou matici $\mathbf{X}$. Když k této matici přičteme matici, která bude mít čtyři st sloupce tvaru $\alpha\,(-1, 1, 0, 0, 0, 0)^T + \beta\,(-3, 0, 0, 1, 0, 0)^T + \gamma\,(1, 0, -2, 0, 1,$ $\alpha, \beta, \gamma \in \mathbf{R}$, dostáváme zápis obecně všech matic $\mathbf{X}$, které vyhovují zad maticové rovnici.

Maticovou rovnici $\mathbf{XA} = \mathbf{B}$ (při daných maticích $\mathbf{A}$, $\mathbf{B}$) bychom ř například tak, že transponujeme obě strany rovnosti. Tím dostáváme $\mathbf{A}^T\mathbf{X}$

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 $\mathbf{EX}$ =
Řešením soustavy $\mathbf{EX} = \mathbf{C}$ je zřejmě matice $\mathbf{C}$. Protože Gaussova elimin
metoda nemění množinu řešení a podle (1) víme, že řešením obou sousta
$\mathbf{A}^{-1}\mathbf{B}$. Takže $\mathbf{C} = \mathbf{A}^{-1}\mathbf{B}$.

Důsledkem této věty je například metoda výpočtu inverzní matice. Inve
matice je podle definice ?? taková matice $\mathbf{X}$, pro kterou platí $\mathbf{AX} = \mathbf{E}$. S
tedy v předchozí větě volit $\mathbf{B} = \mathbf{E}$.

Předpokládejme regulární matici $\mathbf{A} \in \mathbf{R}^{n,n}$ a soustavu lineárních
nic $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$. Jediné řešení této soustavy můžeme počítat ze vzorce $\mathbf{A}^{-1}$
výpočtu matice $\mathbf{A}^{-1}$ eliminací potřebujeme $2n^3$ operací (za jednu operaci
važujeme přičtení násobku jednoho čísla k jinému). A pro maticové násob
$\mathbf{A}^{-1}\boldsymbol{b}$ potřebujeme dalších n^2 operací. Je zřejmé, že přímá úprava rozší
matice eliminací spotřebuje nepatrně méně operací: $n^2(n+1) = n^3 + n^2$
rací. Ještě méně operací potřebujeme při řešení této soustavy LU rozklad
Postup řešení je vysvětlen v následujícím algoritmu.

[LUsoustava] Nechť $\mathbf{A}$ je regulární matice, $\mathbf{AP} = \mathbf{LU}$ je její LU rozk
Pak:

$$\mathbf{A} = \mathbf{LUP}^T, \quad \text{tedy soustavu } \mathbf{A}\boldsymbol{x} = \boldsymbol{b} \text{ lze zapsat ve tvaru } \mathbf{L}\left(\mathbf{U}\left(\mathbf{P}^T\boldsymbol{x}\right)\right) =$$

$$\text{a řešit postupně tři soustavy: } \mathbf{L}\boldsymbol{z} = \boldsymbol{b}, \quad \mathbf{U}\boldsymbol{y} = \boldsymbol{z}, \quad \mathbf{P}^T\boldsymbol{x} =$$

Přitom první a třetí soustavu není nutné řešit, protože algoritmus LU
kladu ?? poskytuje jako vedlejší produkt matici $L' = L^{-1}$ a dále platí
$(\mathbf{P}^T)^{-1}$. Takže řešíme jedinou soustavu $\mathbf{U}\,\boldsymbol{y} = \mathbf{L}'\,\boldsymbol{b}$ a podle permutační ma
$\mathbf{P}$ přehodíme případně pořadí proměnných, tedy provedeme $\boldsymbol{x} = \mathbf{P}\boldsymbol{y}$.

Řešme LU rozkladem soustavu lineárních rovnic s maticí

$$\mathbf{A} = \left(\begin{array}{ccc|c} 1 & 2 & 3 & 5 \\ 2 & 3 & 1 & 7 \end{array}\right)$$

Soustava $\mathbf{U}\,\boldsymbol{y} = \mathbf{L}'\,\boldsymbol{b}$ má rozšířenou matici:

$$\left(\begin{array}{rrr|r} 1 & 2 & 3 & 5 \\ 0 & -1 & -5 & -3 \\ 0 & 0 & 18 & 4 \end{array}\right),$$

kterou vyřešíme postupným dosazením „zespoda nahoru“: $y_3 = \frac{2}{9}$, $y_2 =$
$y_1 = \frac{5}{9}$. Permutační matice $\mathbf{P}$ je v tomto případě jednotková, takže $x_1 =$
$x_2 = y_2$, $x_3 = y_3$ a dostáváme řešení soustavy $(\frac{5}{9}, \frac{17}{9}, \frac{2}{9})$.

Kolik operací (přičtení násobku čísla k jinému) potřebujeme k vyře
soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ s regulární maticí typu (n, n)? K nalezení matic $\mathbf{U}$ a $\mathbf{L}'$
třebuje algoritmus LU rozkladu zhruba $n^3/2$ operací. K výpočtu pravé str
$\boldsymbol{z}$ potřebujeme $n^2/2$ operací a k vyřešení soustavy $\mathbf{U}\boldsymbol{y} = \boldsymbol{z}$ potřebujeme
$n^2/2$ operací. K prohození proměnných (přechod mezi vektorem $\boldsymbol{y}$ a $\boldsymbol{x}$) po
bujeme zhruba n operací, což je ve srovnání s počtem n^2 operací pro výp
$\boldsymbol{y}$ zanedbatelné. Shrnutí: na přípravu matice $\mathbf{A}$ (LU rozklad) je potřeba n
operací a na výpočet řešení pak už stačí n^2 operací.

Zdá se, že počet operací při řešení soustav pomocí LU rozkladu nebo G
sovou eliminační metodou se příliš neliší. Ovšem jsou známy algoritmy LU
kladu se stejnou složitostí jako násobení matic. Přitom násobení matic se
optimalizovat tak, že potřebuje méně operací než n^3 (viz ??). Za určitých o
ností při rozsáhlých soustavách může tedy být řešení soustav LU rozkla
efektivnější.

[nullprst] Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$. *Nulový prostor matice* $\mathbf{A}$ je lineární podpro
všech řešení homogenní soustavy lineárních rovnic $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$. Tento podpro
značíme $\operatorname{Null}\mathbf{A}$.

Je-li dána matice $\mathbf{A}$, pak k ní můžeme sestrojit dva lineární podpros
lineárního prostoru $\mathbf{R}^n$: nulový prostor $\operatorname{Null}\mathbf{A}$ a lineární obal řádků ma
$\langle \mathrm{r}\colon \mathbf{A}\rangle$. Mezi těmito dvěma lineárními podprostory je zajímavý vztah:

Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$. Pak

Důkaz. (1) Rovnost $\boldsymbol{a} \cdot \boldsymbol{x}^T = 0$ můžeme po složkách rozepsat jako $a_1 x$
$a_2 x_2 + \cdots + a_n x_n = 0$ a vnímat ji jako rovnici s koeficienty $\boldsymbol{a} = (a_1, a_2, \ldots,$
Protože $\boldsymbol{a} \in \langle \mathrm{r}\colon \mathbf{A} \rangle$, je $\boldsymbol{a}$ lineární kombinací řádků matice $\mathbf{A}$, tedy uve
rovnice vznikla jako lineární kombinace rovnic ze soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$. Ře
$\boldsymbol{z} \in \operatorname{Null} \mathbf{A}$ splňuje nejen všechny rovnice ze soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{y}$, ale také vše
jejich lineární kombinace, takže platí $a_1 z_1 + a_2 z_2 + \cdots + a_n z_n = 0$.

(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 $x_1 x_1 + x_2 x_2 + \cdot$
$x_n x_n = x_1^2 + x_2^2 + \cdots + x_n^2 = 0$ 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 vět

(4) Předpokládejme, že $\operatorname{hod} \mathbf{A} = k$ a nechť $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$ je nějaká
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
prostoru $\operatorname{Null} \mathbf{A}$. Pak podle věty ?? jsou vektory $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n$ lineárně nezá
a tvoří tedy bázi lineárního prostoru $\mathbf{R}^n$. Vektor $\boldsymbol{x} \in \mathbf{R}^n$ má vzhledem k
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 $\boldsymbol{z}$. J
jednoznačnost plyne z jednoznačnosti souřadnic vzhledem k bázi.

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 matic
Protože $\boldsymbol{a} \cdot \boldsymbol{z}^T = \boldsymbol{z} \cdot \boldsymbol{a}^T = 0$, vidíme, že vektor $\boldsymbol{a}$ řeší homogenní rovn
koeficienty $\boldsymbol{z} = (z_1, z_2, \ldots, z_n)$. Sestavíme matici $\mathbf{B}$, která v řádcích obsa
bázi nulového prostoru matice $\mathbf{A}$. Pak zřejmě $\boldsymbol{a}$ řeší soustavu $\mathbf{B}\boldsymbol{x} = \boldsymbol{o}$. T
nejen $\operatorname{Null} \mathbf{A} = \langle \mathrm{r}\colon \mathbf{B} \rangle$, ale také $\operatorname{Null} \mathbf{B} = \langle \mathrm{r}\colon \mathbf{A} \rangle$.

Množina řešení soustavy lineárních rovnic je dle Frobeniovy věty /
prázdná, právě když hodnost rozšířené matice soustavy je větší než hod
matice soustavy.

Množina řešení homogenní soustavy lineárních rovnic s n neznámými t
lineární podprostor lineárního prostoru $\mathbf{R}^n$ /??/. Dimenze tohoto podpros

jednotlivých rovnic /??, ??/. Je to také zobecněná rovina, která vzniká posu
tím zobecněné roviny popisující množinu řešení přidružené homogenní soust
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 rů
zápisy popisují stejnou množinu řešení.

Soustavy se čtvercovou maticí mají svou matici singulární (pak po el
naci už nemají čtvercovou matici), nebo regulární. Ta má jediné řešení ve tv
$\mathbf{A}^{-1}\boldsymbol{b}$. Jednotlivé složky takového řešení se dají spočítat jako podíl dete
nantů /Cramerovo pravidlo ??/.

Vyřešit maticovou rovnici $\mathbf{AX} = \mathbf{B}$ znamená totéž, jako vyřešit soust
soustav se stejnou maticí soustavy a s různými pravými stranami /??/. El
nace $(\mathbf{A}\,|\,\mathbf{B}) \sim (\mathbf{E}\,|\,\mathbf{C})$ počítá součin $\mathbf{C} = \mathbf{A}^{-1}\,\mathbf{B}$, což je jediné řešení soust
$\mathbf{AX} = \mathbf{B}$ v případě, že matice $\mathbf{A}$ je regulární /??/.

V závěru kapitoly jsme ukázali řešení soustav lineárních rovnic LU roz
dem.

10. Matice lineárního zobrazení

[aA] Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$ je matice. Pak zobrazení $\mathcal{A}\colon \mathbf{R}^n \to \mathbf{R}^m$ definov
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 ??.

Zobrazení v předchozí větě zobrazuje sloupcové vektory na sloupcové
tory, tedy přesněji bychom měli psát $\mathcal{A}\colon \mathbf{R}^{n,1} \to \mathbf{R}^{m,1}$. Ovšem vzhlede
izomorfismu mezi $\mathbf{R}^{n,1}$ a $\mathbf{R}^n$ (viz poznámku ??) nebudeme dále tuto sku
nost zbytečně zdůrazňovat.

[R4toR3] Najdeme jádro, defekt a hodnost zobrazení $\mathcal{A}\colon \mathbf{R}^4 \to \mathbf{R}^3$, k
je dáno předpisem $\mathcal{A}(x_1, x_2, x_3, x_4) = (x_1 + 3x_2 + 2x_3 + 2x_4, 3x_1 + x_2 + 2x_4, 5$
$7x_2 + 4x_3 + 6x_4)$.

Ze vzorce pro hodnotu zobrazení okamžitě plyne, že

$$\mathcal{A}(x_1, x_2, x_3, x_4)^T = \begin{pmatrix} x_1 + 3x_2 + 2x_3 + 2x_4 \\ 3x_1 + x_2 + 2x_4 \\ 5x_1 + 7x_2 + 4x_3 + 6x_4 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 & 2 \\ 3 & 1 & 0 & 2 \\ 5 & 7 & 4 & 6 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

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 p
prostoru všech hodnot zobrazení a tento podprostor je roven lineárnímu o
všech obrazů bázových vektorů. Ve vstupním lineárním prostoru použij
strandardní bázi. Platí

hod $\mathbf{A}^T$, stačí počítat dimenzi lineárního obalu řádků matice $\mathbf{A}$, neboli hod
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 $\boldsymbol{x} \in \mathbf{R}^4$ takov
že $\mathbf{A} \cdot \boldsymbol{x} = \boldsymbol{o}$. Je to tedy lineární podprostor všech řešení homogenní soust
rovnic s maticí $\mathbf{A}$. Řešit soustavy lineárních rovnic umíme:

$$\begin{pmatrix} 1 & 3 & 2 & 2 \\ 3 & 1 & 0 & 2 \\ 5 & 7 & 4 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 2 & 2 \\ 0 & 1 & 3/4 & 1/2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -1/4 & 1/2 \\ 0 & 1 & 3/4 & 1/2 \end{pmatrix} = (\mathbf{E} \,|\, \mathbf{C}$$

$$(-\mathbf{C}^T \,|\, \mathbf{E}) = \begin{pmatrix} 1/4 & -3/4 & 1 & 0 \\ -1/2 & -1/2 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Při výpočtu jsme použili větu ??. $\operatorname{Ker} \mathcal{A} = \langle (1,-3,4,0), (1,1,0,-2) \rangle$, def
$\dim \operatorname{Ker} \mathcal{A} = 2$.

Tento příklad ilustruje lineární zobrazení, které není prosté (protože def
0) a také není „na“ $\mathbf{R}^3$ (protože $\dim \mathbf{R}^3 = 3$, ale $\operatorname{hod} \mathcal{A} = 2$).

[hod=hod] Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$. Hodnost lineárního zobrazení $\mathcal{A} \colon \mathbf{R}^n \to$
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 zobra
v předchozím příkladu. Nechť $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n\}$ je standardní báze lineár
prostoru $\mathbf{R}^n$. Díky vlastnostem maticového násobení je $\mathbf{A} \cdot \boldsymbol{e}_i$ rovno i-t

Věta ?? „def $\mathcal{A}+\operatorname{hod}\mathcal{A}=\dim L_1$“ přechází v případě zobrazení typu A
na větu ?? „$\dim \operatorname{Null}\mathbf{A}+\operatorname{hod}\mathbf{A}=$ počet neznámých soustavy lineárních ro
s maticí $\mathbf{A}$“. Defekt je totiž dimenze kernelu, což je dimenze nulového pros
matice $\mathbf{A}$. Hodnost zobrazení je dle věty ?? rovna hodnosti matice. Kon
$\dim L_1$ je rovna počtu sloupců v matici $\mathbf{A}$, tedy počtu neznámých soustav

V následujícím textu na chvíli opustíme zobrazení typu $\mathbf{A}\cdot\boldsymbol{x}$, abychom
k němu později znovu vrátili obohaceni o další poznatky o obecných lineár
zobrazeních. Pak už budeme moci dokázat, že každé lineární zobrazení lin
ních prostorů konečné dimenze je (až na izomorfismus) zobrazení typu $\mathbf{A}$
kde $\mathbf{A}$ je nějaká matice.

Nechť L_1 a L_2 jsou lineární prostory. Symbolem T označme množinu v
lineárních zobrazení z L_1 do L_2. V následující definici zavedeme součet d
zobrazení, které jsou prvky množiny T, a α-násobek takového zobrazení
větě ?? pak dokážeme, že množina T s těmito operacemi tvoří lineární pros

[lplzob] Nechť $\mathcal{A}\colon L_1\to L_2$, $\mathcal{B}\colon L_1\to L_2$ jsou lineární zobrazení a
$\mathbf{R}$. Pak definujeme součet lineárních zobrazení $\mathcal{A}+\mathcal{B}\colon L_1\to L_2$ předpi
$(\mathcal{A}+\mathcal{B})(\boldsymbol{x})=\mathcal{A}(\boldsymbol{x})+\mathcal{B}(\boldsymbol{x})$ pro všechna $\boldsymbol{x}\in L_1$. Dále definujeme α-náso
zobrazení $\mathcal{A}$ jako zobrazení $\alpha\mathcal{A}\colon L_1\to L_2$, které splňuje $(\alpha\mathcal{A})(\boldsymbol{x})=\alpha\mathcal{A}(\boldsymbol{x})$
všechna $\boldsymbol{x}\in L_1$.

[lpZzob] Nechť L_1 a L_2 jsou lineární prostory a označme $T=\{\mathcal{A}\colon L$
$L_2\}$. Pak T s operacemi podle definice ?? je lineární prostor.

Důkaz. Nejprve je potřeba dokázat, že součet lineárních zobrazení je line
zobrazení a α násobek lineárního zobrazení je také lineární zobrazení. Tedy
ně musí platit vlastnosti (1) a (2) z definice ??. Nechť $\mathcal{A}\in T,\mathcal{B}\in T,\alpha\in$
Pro $\boldsymbol{x}\in L_1,\boldsymbol{y}\in L_1$ a $\gamma\in\mathbf{R}$ platí:

$$(1)\quad (\mathcal{A}+\mathcal{B})(\boldsymbol{x}+\boldsymbol{y})=\mathcal{A}(\boldsymbol{x}+\boldsymbol{y})+\mathcal{B}(\boldsymbol{x}+\boldsymbol{y})=\big(\mathcal{A}(\boldsymbol{x})+\mathcal{A}(\boldsymbol{y})\big)+\big(\mathcal{B}(\boldsymbol{x})+$$
$$=\big(\mathcal{A}(\boldsymbol{x})+\mathcal{B}(\boldsymbol{x})\big)+\big(\mathcal{A}(\boldsymbol{y})+\mathcal{B}(\boldsymbol{y})\big)=(\mathcal{A}+\mathcal{B})(\boldsymbol{x})+($$

Dále je třeba dokázat, že pro operace + a · z definice ?? platí axiomy li
rity, tedy vlastnosti (1) až (7) z definice ??. Argumentace je zcela stejná,
v příkadu ??, takže ji zde nebudeme opakovat. Rozdíl je jen v tom, že se př
gumentaci neopíráme o vlastnosti sčítání a násobení reálných čísel, ale opír
se o axiomy linearity, které platí v lineárním prostoru L_2.

Následující věta ukazuje, že pokud známe hodnoty zobrazení $\mathcal{A}: L_1 -$
jen na bázi lineárního prostoru L_1 a toto zobrazení má být lineární, pak tal
zobrazení existuje a je hodnotami na bázi jednoznačně určeno.

* [zobnabasi] Nechť $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ je báze lineárního prostoru L_1 a n
jsou dány libovolné vektory $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_n$ z lineárního prostoru L_2. Pak exis
právě jedno lineární zobrazení $\mathcal{A}: L_1 \to L_2$, pro které platí

$$\mathcal{A}(\boldsymbol{b}_i) = \boldsymbol{y}_i, \quad \forall i \in \{1, 2, \ldots, n\}.(anabasi)$$

Důkaz. (1) Existence. Nechť $\boldsymbol{x} \in L_1$. Protože $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ je báze
existují souřadnice $\alpha_i \in \mathbf{R}$ vektoru $\boldsymbol{x}$ takové, že $\boldsymbol{x} = \alpha_1 \boldsymbol{b}_1 + \alpha_2 \boldsymbol{b}_2 + \cdots + \alpha_n$
Hodnotu zobrazení $\mathcal{A}$ v bodě $\boldsymbol{x}$ nyní definujeme takto:

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

Zobrazení, které vektorům přiřazuje jejich souřadnice, je lineární (viz větu
Z toho plyne, že zobrazení $\mathcal{A}$ definované vzorcem (??) je lineární. Pečliv
čtenář si to rozepíše podrobněji.

Protože souřadnice vektoru $\boldsymbol{b}_i$ vzhledem k bázi (B) jsou všechny nulo
výjimkou i-té souřadnice, která je rovna jedné, platí

$$\mathcal{A}(\boldsymbol{b}_i) = \sum^{n} 0 \cdot \boldsymbol{y}_j + 1 \cdot \boldsymbol{y}_i = \boldsymbol{y}_i,$$

$\forall i \in \{1, 2, \ldots, n\}$, protože $\mathcal{A}$ i $\mathcal{B}$ splňují vlastnost (??). Z linearity zobra $\mathcal{A} - \mathcal{B}$ 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 $\mathcal{A}$

V důkazu věty ?? jsme uvedli důležitý vzorec (??), který ukazuje, jak n hodnotu lineárního zobrazení pro libovolný vektor $\boldsymbol{x} \in L_1$, známe-li hod tohoto zobrazení jen na nějaké bázi lineárního prostoru L_1.

[R3toR4] Předpokládejme, že $\mathcal{A}\colon \mathbf{R}^3 \to \mathbf{R}^4$ je lineární zobrazení. Najd 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, t podle poznámky ?? bázi lineárního prostoru $\mathbf{R}^3$. Známe hodnoty hleda zobrazení na bázi $\mathbf{R}^3$, takže podle věty ?? můžeme jednoznačně určit hod $\mathcal{A}$ i v ostatních bodech definičního oboru. Budeme postupovat stejně, v důkazu věty ??.

Nechť (x_1, x_2, x_3) je libovolný vektor z $\mathbf{R}^3$. Najdeme souřadnice to 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 šířenou 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

[aRA] Pro každé lineární zobrazení $\mathcal{A}\colon \mathbf{R}^n \to \mathbf{R}^m$ existuje právě je 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 $(S_n) = (\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots$ standardní bázi v $\mathbf{R}^n$. Hodnoty $\mathcal{A}(\boldsymbol{e}_i)$ pro $i = \{1, 2, \ldots, n\}$ zapišme jako sl cové vektory vedle sebe do matice, kterou označíme $\mathbf{A}$. Tedy $\mathbf{A} = \big(\mathcal{A}(\boldsymbol{e}_1)\ \mathcal{A}($ Je zřejmé, že zobrazení, které vektoru $\boldsymbol{x}$ přiřadí vektor $\mathbf{A} \cdot \boldsymbol{x}$, má pro $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n\}$ stejné hodnoty, jako dané zobrazení $\mathcal{A}$. Podle věty ?? exis jediné lineární zobrazení s takovou vlastností.

Proč je matice $\mathbf{A}$ zobrazením $\mathcal{A}$ jednoznačně určena? Jiná matice odpo zobrazení, které má jiné hodnoty pro $\boldsymbol{x} \in \{\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n\}$, takže to je zobrazení.

[defaRA] Nechť $\mathcal{A}\colon \mathbf{R}^n \to \mathbf{R}^m$ je lineární zobrazení. Matici $\mathbf{A}$, pro kt je $\mathbf{A} \cdot \boldsymbol{x} = \mathcal{A}(\boldsymbol{x})\ \forall \boldsymbol{x} \in \mathbf{R}^n$, nazýváme *maticí lineárního zobrazení $\mathcal{A}$*.

Důkaz věty ?? dává návod, jak matici zobrazení $\mathcal{A}$ sestavit. Do slou matice je třeba zapsat obrazy vektorů standardní báze.

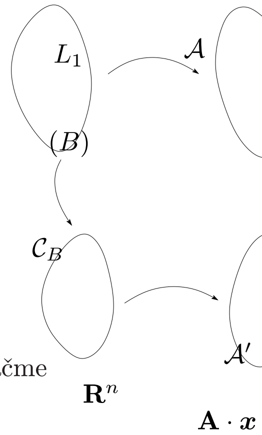
[mR3toR4] V příkladu ?? jsme měli zobrazení $\mathcal{A}\colon \mathbf{R}^3 \to \mathbf{R}^4$ dáno ho tami na bázi a vypočítali jsme, že $\mathcal{A}(x_1, x_2, x_3) = (x_2,\ -4x_1 + 2x_3,\ -2x$ $x_2 + x_3,\ -2x_1 + x_3)$. Nyní najdeme jeho matici, hodnost, jádro a defekt.

Matici můžeme hledat dvěma způsoby. Obrazy bázových vektorů s dardní báze musejí být zapsány postupně do sloupců matice $\mathbf{A}$. Nebo ji koeficienty lineárních kombinací jednotlivých složek obrazu vektoru $(x_1, x_2$ musejí být zapsány do řádků matice $\mathbf{A}$. Vyzkoušejte si oba přístupy. Takž

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 \\ -4 & 0 & 2 \\ -2 & 1 & 1 \\ -2 & 0 & 1 \end{pmatrix}$$

Hodnost zobrazení je rovna hodnosti jeho matice (věta ??), jádro zobraze

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.



* [defAa] 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 $\mathcal{C}_C\colon L_2 \to \mathbf{R}^m$ je izomorfismus, který přiřazuje vektoru $\boldsymbol{v} \in L_2$ jeho souřadnice vzhledem k uspořádané bázi (C). Složené zobrazení $\mathcal{A}' = \mathcal{C}_C \circ \mathcal{A} \circ \mathcal{C}_B^{-}$ zobrazením z $\mathbf{R}^n$ do $\mathbf{R}^m$ a má tedy podle věty ?? svou matici $\mathbf{A} \in \mathbf{R}^{m,n}$. T matici nazýváme *maticí zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C)* a značím $\mathbf{A} = \mathcal{M}_{B,C}(\mathcal{A})$.

* [Aasour] Nechť $\mathcal{A}\colon L_1 \to L_2$ je lineární zobrazení, $\dim L_1 = n$ a $\dim L$ m. Nechť (B) je uspořádaná báze v L_1 a (C) je uspořádaná báze v L_2. N $\mathbf{A} = \mathcal{M}_{B,C}(\mathcal{A})$ je matice zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C). N $\boldsymbol{u} \in L_1$, $\boldsymbol{v} \in L_2$, $\mathcal{A}(\boldsymbol{u}) = \boldsymbol{v}$. Nechť $\boldsymbol{x} = \mathcal{C}_B(\boldsymbol{u})^T$ jsou souřadnice vekto vzhledem k bázi (B) a $\boldsymbol{y} = \mathcal{C}_C(\boldsymbol{v})^T$ jsou souřadnice vektoru $\boldsymbol{v}$ vzhledem k (C). Pak $\mathbf{A} \cdot \boldsymbol{x} = \boldsymbol{y}$. Lapidárně řečeno, pro každé $\boldsymbol{u} \in L_1$ platí:

(souřadnice (souřadnice

Důkaz. Věta je jen v jiné formě zapsaná definice ?? matice lineárního zbra vzhledem k bázím (B) a (C). Zobrazení $\mathcal{A}'$ z této definice zobrazuje souřad vektoru $\boldsymbol{u}$ vzhledem k bázi (B) na souřadnice vektoru $\mathcal{A}(\boldsymbol{u})$ vzhledem k (C), tedy zobrazí $\boldsymbol{x}$ na $\boldsymbol{y}$. Matice $\mathbf{A}$ zobrazení $\mathcal{A}'$ podle definice ?? spl $\mathbf{A} \cdot \boldsymbol{x} = \boldsymbol{y}$.

Obráceně: stačí ukázat, že nemohou existovat dvě různé matice sp jící (??) pro všechna $\boldsymbol{u} \in L_1$. Označme $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ a dosadím rovnosti (??) postupně $\boldsymbol{u} = \boldsymbol{b}_i$. Souřadnice vektoru $\boldsymbol{b}_i$ vzhledem k bázi $(B$ vektor $\boldsymbol{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)^T$, kde jednička je v i-té složce. Maticové sobení $\mathbf{A} \cdot \boldsymbol{e}_i$ je rovno i-tému sloupci matice $\mathbf{A}$. Takže matice $\mathbf{A}$ musí v i- sloupci obsahovat souřadnice vektoru $\mathcal{A}(\boldsymbol{b}_i)$ vzhledem k bázi (C). Taková tice je jenom jediná a je zřejmě maticí zobrazení $\mathcal{A}$ vzhledem k bázím $($ (C).

* [Asloupce] 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 usp daná báze v L_2. Matice $\mathbf{A}$ je maticí zobrazení $\mathcal{A}$ vzhledem k bázím (B) a právě tehdy, když obsahuje v i-tém sloupci souřadnice vektoru $\mathcal{A}(\boldsymbol{b}_i)$ vzhle k bázi (C) pro všechna $i \in \{1, 2, \ldots, n\}$.

Důkaz. Viz druhou část důkazu předchozí věty.

* [matzob] Nechť $\mathcal{A}\colon L_1 \to L_2$ je lineární zobrazení. Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2$ je uspořádaná báze v L_1 a $(C) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m)$ je uspořádaná báze v L_2. tice $\mathbf{A}$ je maticí zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C) právě tehdy, k splňuje maticovou rovnost

$$\big(\mathcal{A}(\boldsymbol{b}_1) \quad \mathcal{A}(\boldsymbol{b}_2) \quad \ldots \quad \mathcal{A}(\boldsymbol{b}_n)\big) = (\boldsymbol{c}_1 \quad \boldsymbol{c}_2 \quad \ldots \quad \boldsymbol{c}_m) \cdot \mathbf{A}.(mzob)$$

Uvedenou rovnost čteme takto: jednořádková matice s obrazy bázových vek

Matici zobrazení jsme definovali jednak v definici ?? a také v definici
Je zřejmé, že matice zobrazení bez uvedení bází (podle definice ??) je z pohl
definice ?? maticí zobrazení vzhledem ke standardním bázím (S_n) v $\mathbf{R}^n$ a (
v $\mathbf{R}^m$. Je to z toho důvodu, že složky vektoru z $\mathbf{R}^n$ jsou podle věty ?? ro
souřadnicím vektoru vzhledem ke standardní bázi.

Domluvíme se na tom, že pokud budeme pracovat s lineárními zobr
ními $\mathbf{R}^n \to \mathbf{R}^m$ a pouze se standardními bázemi v $\mathbf{R}^n$ a $\mathbf{R}^m$, pak nemus
v případě matice zobrazení explicitně mluvit o bázích (jako v definici ??
ostatních případech budeme báze v souvislosti s maticí zobrazení vždy uvá

[derpol] Nechť L_1 je lineární prostor všech polynomů nejvýše třetího stu
a L_2 je lineární prostor všech polynomů nejvýše druhého stupně. Uvažu
zobrazení $\mathcal{A}\colon L_1 \to L_2$, které derivuje polynomy, tedy $\mathcal{A}(p) = p'$. Toto
razení je zřejmě lineární. V lineárním prostoru L_1 zvolme uspořádanou
$(B) = (1, x, x^2, x^3)$ 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: $\mathcal{A}(1) = 0$, $\mathcal{A}(x) = 1$, $\mathcal{A}(x^2) = 2x$, $\mathcal{A}(x$
$3x^2$. Souřadnice těchto obrazů vzhledem k bázi (C) jsou: $\mathcal{C}_C(0) = (0,0$
$\mathcal{C}_C(1) = (1,0,0)$, $\mathcal{C}_C(2x) = (0,2,0)$, $\mathcal{C}_C(3x^2) = (0,0,3)$. Abychom získali ma
zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C), je potřeba podle věty ?? uved
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 a
$bx^2 + cx + d$ má v uspořádané bázi (B) souřadnice (d, c, b, a). Souřadnice
obrazu (tj. v tomto příkladě jeho derivace) vzhledem k uspořádané bázi
najdeme podle věty ?? maticovým násobením:

[bR3toR4] Najdeme matici zobrazení $\mathcal{A}\colon \mathbf{R}^3 \to \mathbf{R}^4$ z příkladu ?? vzhle k uspořádaným bázím (B) a (S_4), kde $(B) = \big((1,1,2),(1,2,2),(2,1,5)\big)$ a je standardní báze v $\mathbf{R}^4$.

Protože souřadnice vektorů z $\mathbf{R}^4$ vzhledem ke standardní bázi S_4 přímo rovny složkám těchto vektorů (viz větu ??), stačí napsat složky obr vektorů z (B) do sloupců matice. Tyto obrazy jsou přímo v zadání příkla

$$\mathcal{M}_{B,S_4}(\mathcal{A}) = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 2 \\ 1 & 2 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Povšimneme si, že k sestavení této matice jsme nepotřebovali znát vzorec $\mathcal{A}(x_1,x_2,x_3)$, stačilo sepsat do sloupců matice údaje, které byly obsahem za příkladu. Na druhé straně k sestavení matice $\mathcal{M}_{S_3,S_4}$ (viz příklad ??) j vzorec pro $\mathcal{A}(x_1,x_2,x_3)$ potřebovali znát.

V mnoha příkladech na lineární zobrazení se setkáváme se zobrazenín stejného lineárního prostoru. Bude tedy užitečné uvést následující definici.

Lineární zobrazení $\mathcal{A}\colon L \to L$ (tj. z lineárního prostoru do *téhož* lineár prostoru) se nazývá *lineární transformace*. Nechť $\mathcal{A}\colon L \to L$ je lineární tr formace, $\dim L = n$. Matici $\mathcal{M}_{B,B}(\mathcal{A}) \in \mathbf{R}^{n,n}$ nazýváme *maticí transform vzhledem k uspořádané bázi* (B). Ušetříme si tedy koktání: místo abychom vili o matici lineárního zobrazení vzhledem k bázím (B) a (B), říkáme struč matice transformace vzhledem k bázi (B).

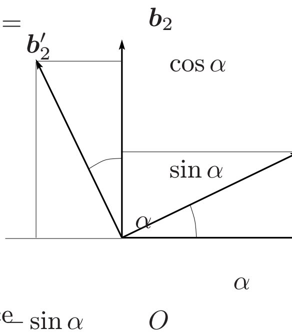
[projekce] V lineárním prostoru U_O orientovaných úseček se společ počátkem O (viz příklad ??) jsou dány tři lineárně nezávislé vektory $\boldsymbol{b}_1, \boldsymbol{b}_2$ Uvažujme transformaci $\mathcal{A}\colon U_O \to U_O$, která každé orientované úsečce při její stín na rovině procházející vektory $\boldsymbol{b}_2, \boldsymbol{b}_3$, přitom světelné paprsky 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. ideme matici $\mathcal{M}_{B,B}(\mathcal{A})$ transformace $\mathcal{A}$ vzhledem k uspořádané bázi (B)

má vektor $\boldsymbol{u} \in U_O$ se souřadnicemi (x, y, z) svůj stín, který má souřad
$(0, y, z)$.

[rotace] V lineárním prostoru U_O orientovaných úseček s počátkem v b
O (viz příklad ??) zvolme podprostor P dimenze 2 (vektory ležící ve spole
rovině). V tomto prostoru P zvolme bázi $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2)$ tak, že vektory b
jsou na sebe kolmé a mají jednotkovou velikost (jako na obrázku níže). Tr
formaci, která otočí každý vzor o pevně zvolený úhel α označíme $\mathcal{R}_\alpha : P \to$
budeme jí říkat *rotace*. Najdeme matici $\mathcal{M}_{B,B}(\mathcal{R}_\alpha)$ této transformace vzhle
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 druh
sloupce hledané matice. Dostáváme

$$\mathcal{M}_{B,B}(\mathcal{R}_\alpha) = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \ldots \end{pmatrix}$$

Souřadnice otočeného vektoru vzhledem k bázi (B) tedy jsou (x', y'), kde

$$
\begin{aligned}
x' &= x\cos\alpha - y\sin\alpha,\\
y' &= x\sin\alpha + y\cos\alpha.
\end{aligned}
$$

* [hodhod] Nechť $\mathcal{A}\colon L_1 \to L_2$ je lineární zobrazení prostorů kone dimenze, nechť $\mathbf{A}$ je jeho matice vzhledem k nějaké bázi (B) v L_1 a bázi (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 definic 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 $\mathcal{C}_C^{-1} \circ \mathcal{A}' \circ \mathcal{C}_B$. Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je báze v L_1 a $(S_n) = (\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots$ je standardní báze v $\mathbf{R}^n$. Platí $\boldsymbol{e}_i = \mathcal{C}_B(\boldsymbol{b}_i)$. Nyní spočítejme $\operatorname{hod}\mathcal{A}$:

$$
\begin{aligned}
\operatorname{hod}\mathcal{A} &= \dim\mathcal{A}(L_1) = \dim\mathcal{A}\big(\langle \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\rangle\big) = \dim\big\langle \mathcal{A}(\boldsymbol{b}_1), \mathcal{A}(\boldsymbol{b}_2), \ldots, \mathcal{A}(\\
&= \dim\big\langle \mathcal{C}_C^{-1} \circ \mathcal{A}' \circ \mathcal{C}_B(\boldsymbol{b}_1),\ \mathcal{C}_C^{-1} \circ \mathcal{A}' \circ \mathcal{C}_B(\boldsymbol{b}_2),\ \ldots,\ \mathcal{C}_C^{-1} \circ \mathcal{A}' \circ \mathcal{C}_B(\boldsymbol{b}_n\\
&= \dim \mathcal{C}_C^{-1}\big(\big\langle \mathcal{A}'(\boldsymbol{e}_1), \mathcal{A}'(\boldsymbol{e}_2), \ldots, \mathcal{A}'(\boldsymbol{e}_n)\big\rangle\big) \overset{\star}{=} \dim\big\langle \mathcal{A}'(\boldsymbol{e}_1), \mathcal{A}'(\boldsymbol{e}_2), \ldots\\
&= \dim\mathcal{A}'\big(\langle \boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n\rangle\big) = \dim\mathcal{A}'(\mathbf{R}^n) = \operatorname{hod}\mathcal{A}'
\end{aligned}
$$

Rovnost označená hvězdičkou platí kvůli tomu, že $\mathcal{C}_C^{-1}$ je isomorfismus, t zachovává dimenzi lineárních podprostorů.

[regultransf] Lineární transformace prostoru konečné dimenze je pr právě tehdy, když má regulární matici.

Důkaz. Lineární transformace $\mathcal{A}\colon L \to L$ je prostá právě když má nu defekt (viz větu ??). To platí právě tehdy, když $\operatorname{hod}\mathcal{A} = \operatorname{hod}\mathbf{A} = \dim L$ (viz věty ?? a ??). Matice $\mathbf{A} \in \mathbf{R}^{n,n}$ transformace $\mathcal{A}$ je regulární právě te

Hodnost zobrazení $\mathcal{A}$ je rovna podle věty ?? hodnosti jeho matice. jsme sestavili v příkladu ??. Matice zobrazení má hodnost 2, tedy i hod $\mathcal{A}$ Defekt zobrazení $\mathcal{A}$ spočítáme podle vzorce $\operatorname{def} \mathcal{A} + \operatorname{hod} \mathcal{A} = \dim L_1 = 3$, t def $\mathcal{A} = 1$.

Toto zobrazení tedy převede 3D vzor ($\dim L_1 = 3$) na 2D obraz (hod 2), tedy při tomto zobrazení ztrácíme informace z jedné dimenze (def $\mathcal{A}$ = To vysvětluje, proč se tomuto zobrazení říká projekce. S tímto slovem se čtenář setkal v souvislosti s promítáním filmů.

Protože matice z příkladů ?? a ?? jsou maticemi stejného lineárního razení (jen vzhledem k různé bázi v L_1), mají hodnost rovnu hodnosti to zobrazení. Tím je zaručeno, že tyto matice mají stejnou hodnost. Z výsle příkadu ?? víme, že tyto matice mají hodnost 3.

Matice rotace z příkladu ?? je regulární, protože $\det \mathcal{M}_{B,B}(\mathcal{R}_\alpha) = \cos^2$ $\sin^2 \alpha = 1$. Podle věty ?? je tedy rotace prostá transformace.

[scale] Budeme pracovat se stejným lineárním podprostorem P orient ných úseček jako v příkladu ?? a zvolíme stejnou uspořádanou bázi (B). Zvo dále čísla $a \in \mathbf{R}$, $b \in \mathbf{R}$. Popíšeme transformaci $\mathcal{S}_{a,b} : P \to P$, která má ma

$$\mathbf{A} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} (mscale)$$

vzhledem k bázi (B). Po použití věty ?? vidíme, že vektor $\boldsymbol{u} \in P$ se sou nicemi (x, y) se zobrazí na vektor se souřadnicemi (ax, by). Co to geometr znamená pro různé parametry a, b?

Při $a = 1$ a $b = 1$ zobrazení $\mathcal{S}$ ponechává vektor $\boldsymbol{u}$ beze změny. Ta transformaci říkáme *identita*.

V případě $a = -1$ a $b = 1$ zobrazení $\mathcal{S}$ transformuje vektor $\boldsymbol{u}$ na jeho o souměrný protějšek podle osy, která prochází vektorem $\boldsymbol{b}_2$. V případě $a =$ $b = -1$ zobrazení $\mathcal{S}$ transformuje vektor $\boldsymbol{u}$ na jeho osově souměrný prot

zde máme v množině vzorů i obrazů o jednu dimenzi méně než v příkladu
Je hod $\mathcal{S} = 1$ a def $\mathcal{S} = 1$.

V případě $a > 0$ a $b = 1$ je obraz a-krát deformován ve směru vektoru
V případě $a = 1$ a $b > 0$ je obraz b-krát deformován ve směru vektoru $\boldsymbol{b}$
případě $a > 0$ a $b > 0$ je obraz deformován v obou směrech. Takové transfor
říkáme *změna měřítka*. Při $a = b$ této transformaci říkáme *stejnolehlost*.

Obecný případ $a \in \mathbf{R}$ a $b \in \mathbf{R}$ odpovídá transformaci změny mě
případně složenou s osovou nebo středovou souměrností. Při $a = 0$ nebo b
je $\mathcal{S}$ projekce. Při $a = 0$ i $b = 0$ je $\mathcal{S}$ zobrazení, které každému vektoru při
nulový vektor. Defekt tohoto zobrazení je 2 a hodnost nula.

Zobrazení $\mathcal{S}_{a,b}\colon P \to P$ s maticí (??) budeme nadále říkat *změna
řítka*. Pod tímto pojmem budeme zahrnovat i všechny speciální případy
vyjmenované.

* [aisoA] Nechť L_1 a L_2 jsou lineární prostory, $\dim L_1 = n$, $\dim L_2 =$
Lineární prostor všech lineárních zobrazení z L_1 do L_2 je izomorfní s lineár
prostorem matic $\mathbf{R}^{m,n}$.

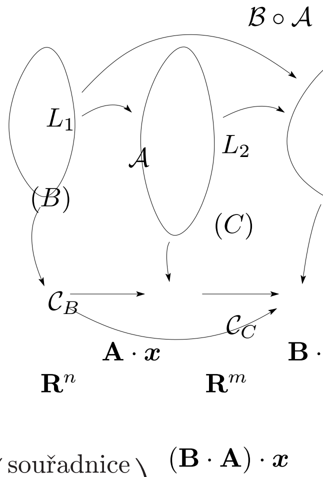
Důkaz (pro hloubavé čtenáře). Označme T lineární prostor všech lineár
zobrazení z L_1 do L_2. Zvolme nějakou uspořádanou bázi v L_1 a označm
(B). Také označme (C) uspořádanou bázi v L_2. (viz též obrázek u definice
Ukážeme, že zobrazení $\mathcal{M}_{B,C}\colon T \to \mathbf{R}^{m,n}$, které přiřazuje zobrazením
jejich matice vzhledem k bázím (B) a (C), je izomorfismus.

Obrazy zobrazení $\mathcal{M}_{B,C}$ jednoznačně existují pro všechna $\mathcal{A} \in T$, pro
každému $\mathcal{A}$ je jednoznačně přiřazeno $\mathcal{A}' = \mathcal{C}_C \circ \mathcal{A} \circ \mathcal{C}_B^{-1}$ a každému takov
$\mathcal{A}'\colon \mathbf{R}^n \to \mathbf{R}^m$ 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 (??), ve k
vidíme, že matice $\mathbf{A}$ udává hodnoty zobrazení $\mathcal{A}$ na bázi (B). Podle vět
existuje jediné lineární zobrazení s takto určenými hodnotami na bázi.

jeho matici je izomorfismus. To je důvod, proč často matematik napíše mat
myslí přitom na lineární zobrazení nebo naopak, pracuje s lineárním zobraze
a hledá k němu matici.

* [slozmzob] 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 zobra $\mathcal{B}\circ\mathcal{A}$ vzhledem k bázím (B) a (D).

Větu ?? můžeme stručně zapsat takto:

$$\mathcal{M}_{B,D}(\mathcal{B}\circ\mathcal{A}) = \mathcal{M}_{C,D}(\mathcal{B})\cdot\mathcal{M}_{B,C}(\mathcal{A})(sloz)$$

[Aainvers] Nechť L je lineární prostor konečné dimenze a (B) je jeho u
řádaná báze. Nechť $\mathcal{A}\colon L \to L$ je prostá lineární tranformace. Pak $\mathcal{A}$ je izo

transformace $\mathcal{A}$ je nejen prostá, ale i „na“ L, tedy je to izomorfismus. Symbo
$\mathcal{I}$ označme identické zobrazení na L. Pro $\mathcal{A}^{-1}$ platí $\mathcal{I} = \mathcal{A}^{-1} \circ \mathcal{A}$. Podle vět
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 ?? r
lární, takže můžeme maticí $\left(\mathcal{M}_{B,B}(\mathcal{A})\right)^{-1}$ vynásobit uvedenou rovnost zpr
Tím dostáváme dokazovaný vztah.

Budeme pracovat v lineárním prostoru P s uspořádanou bází (B) ja
příkladu ??. Lineární transformace $\mathcal{A}\colon P \to P$ otočí vzor o stanovený úh
a následně jej promítne na přímku procházející vektorem $\boldsymbol{b}_2$. Najdeme m
této transformace.

Platí $\mathcal{A} = \mathcal{S}_{0,1} \circ \mathcal{R}_\alpha$, kde $\mathcal{S}_{0,1} : P \to P$ je projekce a $\mathcal{R}_\alpha : P \to P$ je ro
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

$$\mathcal{M}_{B,B}(\mathcal{A}) = \mathcal{M}_{B,B}(\mathcal{S}_{0,1}) \cdot \mathcal{M}_{B,B}(\mathcal{R}_\alpha) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} = ($$

Má-li vektor $\boldsymbol{u}$ souřadnice (x, y) vzhledem k (B), pak $\mathcal{A}(\boldsymbol{u})$ má vzhledem k
souřadnice (x', y'):

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ \sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ (\sin\alpha)\, x + (\cos\alpha)\, y \end{pmatrix}$$

Osovou souměrnost podle p vytvoříme složením tří zobrazení: nejprve číme přímku p o úhel $-\alpha$. Její obraz tedy prochází vektorem $\boldsymbol{b}_1$. Dále proved osovou souměrnost podle přímky procházející vektorem $\boldsymbol{b}_1$ a nakonec oto obraz přímky na své místo otočením o úhel α. Matice jednotlivých transfor vzhledem k bázi (B) jsou

$$\mathcal{M}_{B,B}(\mathcal{R}_{-\alpha}) = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}, \quad \mathcal{M}_{B,B}(\mathcal{S}_{1,-1}) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathcal{M}_{B,B}$$

Hledaná matice osové souměrnosti podle přímky p je součinem těchto mati správném pořadí:

$$\mathcal{M}_{B,B}(\mathcal{A}) = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} = \begin{pmatrix} \cos^2\alpha - \\ 2\cos\alpha \end{pmatrix}$$

Podle vzorečků o dvojnásobném úhlu můžeme výslednou matici přepsat 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 o souměrný obraz podle přímky p má vzhledem k bázi (B) souřadnice $(x', y$

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} (\cos 2\alpha)\, x + (\sin 2\alpha)\, y \\ (\sin 2\alpha)\, x - (\cos 2\alpha)\, y \end{pmatrix}$$

* [defprech] 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 uspořádané báze lineárního prostoru L. Podle věty ?? existuje jediná line transformace $\mathcal{A}\colon L \to L$ taková, že $\mathcal{A}(\boldsymbol{b}_i) = \boldsymbol{c}_i$ pro všechna $i \in \{1, 2, \ldots$ Matici $\mathcal{M}_{B,B}(\mathcal{A})$ transformace $\mathcal{A}$ vzhledem k bázi (B) nazýváme *maticí* *chodu od báze (B) k bázi (C)* a značíme ji $\mathbf{P}$

(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
(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
razů $\mathcal{A}(\boldsymbol{b}_i) = \boldsymbol{c}_i$ vzhledem k bázi (B), kde $\mathcal{A}\colon L \to L$ je lineární transforn
z definice ??.

(2) Rozepsáním součinu $(\boldsymbol{c}_1\ \boldsymbol{c}_2\ \ldots\ \boldsymbol{c}_n) = (\boldsymbol{b}_1\ \boldsymbol{b}_2\ \ldots\ \boldsymbol{b}_n) \cdot \mathbf{P}_{B\to C}$ po sl
cích matice $\mathbf{P}_{B\to C}$ shledáváme, že je tento součin ekvivalentní s (1).

(3) Vzorec (2) lze psát jako $\big(\mathcal{I}(\boldsymbol{c}_1)\ \mathcal{I}(\boldsymbol{c}_2)\ \ldots\ \mathcal{I}(\boldsymbol{c}_n)\big) = (\boldsymbol{b}_1\ \boldsymbol{b}_2\ \ldots$
$\mathbf{P}_{B\to C}$ a dívat se na něj úhlem pohledu vzorce (??), kde $\mathcal{A} = \mathcal{I}$, a kde
prohozeny báze (B) a (C).

(4) plyne z (3) a z věty ??.

Povšimneme si opačného pořadí bází ve vlastnostech (3) a (4) v předc
větě. Vlastnost (4) říká, že matice přechodu od báze (B) k bázi (C) um
počítat souřadnice vektoru vzhledem k bázi (B), pokud jeho souřadnice zn
vzhledem k bázi (C). Je zde tedy opačný směr toku informace, než by
plývalo z názvu matice. Název matice je odvozen z vlastnosti (2), tj. ma
transformuje pomocí maticového násobení bázi (B) na bázi (C).

Všechny vlastnosti ve větě ?? jednoznačně určují matici přechodu $\mathbf{P}_{E}$
Jinými slovy každá z nich by se dala použít jako definice pojmu matice
chodu. Je to tím, že každá podmínka vymezuje matici $\mathbf{P}_{B\to C}$ jednoznač
ve větě ?? jsme dokázali, že tato jediná matice je maticí přechodu od báze
k bázi (C).

(1) Vztah vyplyne například vynásobením rovnosti (2) ve větě ?? ma $(\mathbf{P}_{B\to C})^{-1}$ zprava.

(2) Užitím vzorce (??) a vlastnosti (3) věty ?? dostáváme:

$$\mathbf{P}_{B\to C}\cdot\mathbf{P}_{C\to D}=\mathcal{M}_{C,B}(\mathcal{I})\cdot\mathcal{M}_{D,C}(\mathcal{I})=\mathcal{M}_{D,B}(\mathcal{I})=\mathbf{P}_{B\to D}.$$

* [aprechod] Odvodíme algoritmus na efektivní sestavení matice přech vzhledem k libovolným bázím. Pravda, vlastnost (1) věty ?? dává návod, matici přechodu sestavit. Ovšem někdy se stává, že se souřadnice vzhlede bázi (B) obtížně hledají.

Najdeme v lineárním prostoru L nějakou bázi, vzhledem ke které se řadnice dobře hledají a označíme ji (S). Báze (S) může být standardní bá $\mathbf{R}^n$, báze $(1,x,x^2,x^3)$ v lineárním prostoru polynomů nejvýše třetího stu báze orientovaných úseček jednotkové velikosti a na sebe kolmých v lineár prostoru U_O atd.

Nechť jsou dány báze (B) a (C) v lineárním prostoru L. Pro výp matice přechodu od báze (B) k bázi (C) použijeme vzorce z předchozí vět

$$\mathbf{P}_{B\to C}=\mathbf{P}_{B\to S}\cdot\mathbf{P}_{S\to C}=(\mathbf{P}_{S\to B})^{-1}\cdot\mathbf{P}_{S\to C}.$$

Přitom matice na pravé straně rovnosti sestavíme snadno: do sloupců ma $\mathbf{P}_{S\to B}$ napíšeme souřadnice vektorů báze (B) vzhledem k (S) a do slou matice $\mathbf{P}_{S\to C}$ napíšeme souřadnice vektorů báze (C) vzhledem k (S).

Abychom si ještě ušetřili práci s výpočtem inverzní matice a následn maticovým násobením, použijeme větu ??, která říká $(\mathbf{A}\,|\,\mathbf{B})\sim(\mathbf{E}\,|\,\mathbf{A}^{-1}$ 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 (vedle svislé čáry ještě souřanice báze (C) vzhledem k bázi (S). Po elminin která převede levý blok matice na jednotkovou matici, dostáváme v pra

Najdeme matici přechodu od (B) k (C). Je zřejmé, že souřadnice polynom
nám dobře počítají vzhledem k bázi (S), takže zapíšeme-li do sloupců sou
nice vektorů z báze (B) vzhledem k (S), dostáváme okamžitě $\mathbf{P}_{S\to B}$. Podo
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 $\mathbf{P}_{B\to C}$.

$$(\mathbf{P}_{S\to B} \,|\, \mathbf{P}_{S\to C}) = \left(\begin{array}{cccc|cccc} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 3 & 0 & 0 & 1 & 0 \\ 1 & 1 & 2 & 3 & 0 & 1 & 0 & 0 \\ 1 & -1 & 1 & 1 & 1 & 1 & 2 & 3 \end{array}\right) \sim \left(\begin{array}{cccc|cc} 1 & 0 & 0 & 0 & 1/2 & 1 \\ 0 & 1 & 0 & 0 & -1/2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right.$$

Báze (S), (B) a (C) vymezují v tomto příkladě tři souřadnicové syst
stejného lineárního prostoru. Vezmene nyní jeden vektor (polynom) p d
vzorcem $p(x) = 2x^3 + x^2 - 3x$. Zapíšeme postupně souřadnice tohoto polyn
ve všech třech souřadnicových sytémech.

Souřadnice polynomu p vzhledem k (S) odhalíme snadno: $\mathcal{C}_S(p) = (2, 1$
Zkusíme nyní najít jeho souřadnice vzhledem k bázi (C). Podle vzorce
věty ?? k tomu potřebujeme matici $\mathbf{P}_{C\to S}$. Tu získáme jako inverzi k ma
$\mathbf{P}_{S\to C}$:

$$\mathbf{P}_{C\to S} = (\mathbf{P}_{S\to C})^{-1} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 2 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} -3 & -2 & -1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Od souřadnic polynomu p vzhledem k bázi (C) k souřadnicím vzhledem k
(B) přejdeme pomocí maticového násobení maticí $\mathbf{P}_{B\to C}$. Tu jsme spoč
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
(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 procv
si změny souřadnicového systému za použití maticového násobení. Výsle
můžeme srovnat s příkladem ??, ve kterém jsme počítali totéž, ale souřad
jsme hledali jako řešení soustavy lineárních rovnic.

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 $\boldsymbol{u} \in \mathbf{R}^3$ vzhlede
bázi (B) na jeho souřadnice vzhledem k bázi (C). Dané souřanice vzhlede
bázi (B) označíme (x, y, z). Hlednané souřadnice vzhledem k bázi (C) označ
(x', y', z'). Pro přechod ze souřadnic vektoru vzhledem k bázi (B) k souřa
cím vzhledem k bázi (C) potřebujeme matici přechodu $\mathbf{P}_{C\to B}$. Tu vypočít

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 $x' = -x + \frac{1}{2}y + \frac{1}{2}z,\ y' = \frac{3}{4}y + \frac{5}{4}z,\ z' = x - \frac{1}{4}y - \frac{3}{4}z.$

* [zmenabase] Nechť $\mathcal{A}\colon L_1 \to L_2$ je lineární zobrazení lineárních prost konečné dimenze. Nechť (B) a (B') jsou dvě báze v L_1 a dále něchť (C) a 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 $\mathcal{I}_1: L_1 \to L_1$ je identita na L_1 a $\mathcal{I}_2: L_2 \to L_2$ je identita L_2. Platí $\mathcal{I}_2 \circ \mathcal{A} = \mathcal{A} = \mathcal{A} \circ \mathcal{I}_1$. V důkazu použijeme vzorec (??) a vlastnost 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).

[algA] Podobně, jako v případě algoritmu ??, odvodíme algoritmus na lezení matice zobrazení $\mathcal{A}\colon L_1 \to L_2$ vzhledem k libovolným bázím. Zvolím bázi (S) lineárního prostoru L_2, vzhledem ke které se souřadnice dobře hle 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 $\mathcal{M}_{B,S}(\mathcal{A})$ o

Dostáváme následující algoritmus:

Do sloupců napíšeme pod sebe souřadnice vektorů $\boldsymbol{c}_i$ vzhledem k
vpravo od nich vedle svislé čáry napíšeme do sloupců souřadnice vektorů $\mathcal{A}$
vzhledem k (S). Pak matici eliminujeme tak, abychom v levé části dostal
V pravé části pak máme matici zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C).

Je dáno lineární zobrazení $\mathcal{A}\colon L_1 \to L_2$, které derivuje polynomy, st
jako v příkladu ??. Dále jsou dány báze:

$$(B) = (1, x{+}1, x^2{+}2, x^3{+}3) \quad \text{v prostoru } L_1, \qquad (C) = (x^2{+}3, x{-}2, x^2{-}x)$$

Najdeme $\mathcal{M}_{B,C}(\mathcal{A})$, tedy matici zobrazení $\mathcal{A}$ vzhledem k bázím (B) a
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 slou
matice a tím dostáváme matici $\mathcal{M}_{B,S}(\mathcal{A})$. Matici $\mathbf{P}_{S\to C}$ sestavíme tak, ž
sloupců zapíšeme souřadnice báze (C) vzhledem k bázi (S).

$$\big(\mathbf{P}_{S\to C}\,|\,\mathcal{M}_{B,S}(\mathcal{A})\big) = \left(\begin{array}{rrr|rrrr} 1 & 0 & 1 & 0 & 0 & 0 & 3 \\ 0 & 1 & -1 & 0 & 0 & 2 & 0 \\ 3 & -2 & 0 & 0 & 1 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{rrr|rr} 1 & 0 & 0 & 1/5 & 4 \\ 0 & 1 & 0 & -1/5 & 6 \\ 0 & 0 & 1 & -1/5 & -4 \end{array}\right.$$

Pokud jsou dány hodnoty lineárního zobrazení na bázi (B), ale není zn
vzorec pro výpočet hodnoty v libovolném bodě, pak podle věty ?? line
zobrazení $\mathcal{A}$ s danou vlastností existuje a je právě jedno. Můžeme okam
sestavit matici $\mathcal{M}_{B,S}(\mathcal{A})$. Pokud chceme najít vzorec pro toto zobrazen
libovolném bodě $\boldsymbol{x}$ a chceme pracovat se souřadnicemi $\boldsymbol{x}$ vzhledem k (S)
je obvyklé), je potřeba na matici $\mathcal{M}_{B,S}(\mathcal{A})$ uplatnit přechod od báze (B) k
neboli použít vzorec (1) věty ??. Předvedeme si to na zobrazení $\mathcal{A}\colon \mathbf{R}^3 \to$

V příkladu ?? jsme na základě těchto údajů sestavili matici $\mathcal{M}_{B,S_4}(\mathcal{A})$,
(S_4) je standardní báze v $\mathbf{R}^4$. Nyní potřebujeme provést ještě přechod od
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 uše
výpočet inverzní 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 opač
pořadí, takže musíme přejít k transponovaným maticím:

$$\mathcal{M}_{S_3,S_4}(\mathcal{A})^T = (\mathbf{P}^T_{S_3\to B})^{-1}\cdot\mathcal{M}_{B,S_4}(\mathcal{A})^T, \quad \text{takže:} \quad \big(\mathbf{P}^T_{S_3\to B}\,|\,\mathcal{M}_{B,S_4}(\mathcal{A})^T\big)$$

Z toho plyne algoritmus: tentokrát *do řádků* pod sebe napíšeme složky bázov
vektorů z (B) a vpravo od nich vedle svislé čáry zapíšeme *do řádků* slo
obrazů báze. Po eliminaci, kdy vlevo je jednotková matice, najdeme vp
transponovanou matici $\mathcal{M}_{S_3,S_4}(\mathbf{A})$.

$$\left(\begin{array}{ccc|cccc} 1 & 1 & 2 & 1 & 0 & 1 & 0 \\ 1 & 2 & 2 & 2 & 0 & 2 & 0 \\ 2 & 1 & 5 & 1 & 2 & 2 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|cccc} 1 & 0 & 0 & 0 & -4 & -2 & -2 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 2 & 1 & 1 \end{array}\right) = \big(\mathbf{E}\,|\,\mathcal{M}$$

Náš výsledek se shoduje s výsledkem příkladu ??. Ovšem na rozdíl od postu
příkladu ?? jsme nyní nemuseli počítat vzorec pro $\mathcal{A}(x_1,x_2,x_3)$. Naopak, výs
z právě odvozeného algoritmu se dá použít k sestavení hledaného vzorce
$\mathcal{A}(x_1,x_2,x_3)$, protože platí

$$\mathcal{A}(x_1,x_2,x_3)^T = \mathcal{M}_{S_3,S_4}(\mathcal{A}) \cdot \begin{pmatrix} x_1 \\ x_2 \\ \end{pmatrix}.$$

Lineární zobrazení z L_1 do L_2 lze mezi sebou sčítat a lze je násobit stantou, přičemž tato lineární zobrazení s uvedenými operacemi tvoří line prostor /??, ??/.

Jsou-li dány hodnoty na bázi, existuje právě jedno lineární zobrazení, k má tyto hodnoty /??/.

Nechť L_1 má konečnou uspořádanou bázi (B) a L_2 má konečnou usp danou bázi (C). Každé lineární zobrazení $\mathcal{A}\colon L_1 \to L_2$ lze jednoznačně re zentovat maticí $\mathbf{A}$ takovou, že platí $\mathbf{A} \cdot \boldsymbol{x} = \boldsymbol{y}$, kde $\boldsymbol{x}$ jsou souřadnice v vzhledem k bázi (B) a $\boldsymbol{y}$ jsou souřadnice obrazu vzhledem k bázi (C). T 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 razů báze (B) vzhledem k bázi (C) /??/. Totéž lze vyjádřit maticovým n benním /??/.

Hodnost zobrazení $\mathcal{A}$ je rovna hodnosti jeho matice $\mathbf{A}$ /??, ??/. Souřad všech vektorů jádra zobrazení jsou množinou řešení homogenní soustavy ro $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$.

Přiřazení, které lineárnímu zobrazení přidělí jeho matici vzhledem k pe zvoleným bázím, je izomorfismus /důkaz věty ??/.

Matice složeného zobrazení $\mathcal{B} \circ \mathcal{A}$ je rovna součinu jejich matic $\mathbf{B} \cdot$ stejném pořadí /??/. Matice inverzní transformace je rovna inverzní m původní tansformace /??/.

Matice přechodu $\mathbf{P}_{B \to C}$ od báze (B) k bázi (C) je maticí transform která zobrazí $\boldsymbol{b}_i$ z báze (B) na $\boldsymbol{c}_i$ z báze (C) /??/. Obsahuje ve sloup souřadnice vektorů $\boldsymbol{c}_i$ vzhledem k bázi (B) a je rovna matici identity vzhlede bázím (C) a (B) /??/. Matice $\mathbf{P}_{B \to C}$ umožní transformovat souřadnice vek $\boldsymbol{x}$ 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, pohne

11. Afinní transformace, matice v homogenních souřad-
cích

V desáté kapitole jsme se setkali s maticemi transformací otočení /?
změny měřítka /??/. Do této skupiny tranformací řadíme ještě transforn
posunutí, která ale není lineární, protože nulový vektor „posune“ na n
lový vektor, což způsobně vychované lineární zobrazení kvůli větě ?? neo
Složením transformace posunutí s lineární transformací dostáváme tzv. *a*
transformaci.

Afinní transformace tedy nemá obecně svoji matici. V následujícím t
ukážeme, že při použití speciálních souřadnic (tzv. *homogenních souřadni*
možné sestavit i matice všech afinních transformací a pracovat s nimi st
jako s maticemi lineárních transformací. Tyto matice je možné v případě slo
afinní transformace mezi sebou násobit. To má praktické využití napříkla
programování transformací v počítačové grafice.

[Aprst] Nejprve si upřesníme vlastnosti geometrického prostoru, ve kte
budeme uvedené transformace uplatňovat. Tento prostor nazveme *afinn*
něm budeme rozlišovat objekty dvou typů: *body* a *vektory*. Množinu všech b
budeme značit **X**. Do exaktního zavedení množiny **X** se nebudeme pouštět, s
snad inuitivní chápání pojmu bod.

Vektor je určen orientovanou úsečkou, která je vymezena dvěma body
počátečním a koncovým. Na rozdíl od lineárního prostoru U_O z příkladu ??
nutné, aby orientovaná úsečka začínala v počátku. Navíc považujeme dvě
entované úsečky za reprezentanty stejného vektoru, pokud jsou rovnobě
stejně velké a stejně orientované. Součet dvou vektorů provedeme jako
neárním prostoru U_O, když si narýsujeme jejich orientované úsečky tak,
začínaly ve společném bodě a doplníme na rovnoběžník. Násobek vektoru
stantou provedeme také obdobně jako v lineárním prostoru U_O. Množinu v

* [defAprst] *Afinní prostor* je množina bodů $\mathbf{X}$ společně s lineárním storem vektorů V. Zapisujeme jej jako dvojici $(\mathbf{X}, V)$.

Kromě operací $+ : V \times V \to V$ a $\cdot : \mathbf{R} \times V \to V$ splňující axiomy linearity až (7) definice ?? je zavedena ještě operace $+ : \mathbf{X} \times V \to \mathbf{X}$ 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 $\boldsymbol{u} \in$

(3) pro všechny body $P \in \mathbf{X}$, $Q \in \mathbf{X}$ existuje právě jeden vektor $\boldsymbol{u} \in V$ ta

Definice afinního prostoru je zavedena pomocí axiomů nové operace, je v algebře obvyklé. Nemusíme se tedy obtěžovat přesným vymezením po bod z množiny $\mathbf{X}$ a vektor z množiny V. Také nemusíme vědět, jak konkr pracuje operace „bod plus vektor“. Stačí, že tato operace splňuje uvedené omy.

Z axiomů plyne, že „vektorů je stejný počet jako bodů“. Přesněji, lze n prosté zobrazení z množiny bodů na množinu vektorů. Stačí zvolit jeden $Q \in \mathbf{X}$ a dále pro všechna $P \in \mathbf{X}$ existuje podle axiomu (3) jediný ve $\boldsymbol{u} \in V$. Tím je určeno prosté zobrazení z množiny bodů do množiny vekt Že je toto zobrazení „na“ plyne z toho, že ke každému vektoru $\boldsymbol{u} \in V$ lze zp sestrojit bod $P = Q + \boldsymbol{u}$.

V dalším textu si vystačíme s představou geometrického prostoru s in tivním pojetím bodů a vektorů podle poznámky ??. Ukážeme, že tato předst je v souladu s definicí ??. Tj. ověříme platnost axiomů pro operaci sčítání b P s vektorem $\boldsymbol{u}$ zavedenou geometricky: $P + \boldsymbol{u}$ je koncový bod orientov úsečky vektoru $\boldsymbol{u}$, která začíná v bodě P.

Axiom (1): Vektor $\boldsymbol{o}$ má koncový bod ve stejném místě jako počáte Takže operace $P + \boldsymbol{o}$ bod P nezmění.

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 ?

Souřadnicový systém v afinním prostoru $(\mathbf{X}, V)$ zavedeme tak, že zvo nějakou uspořádanou bázi (B) lineárního prostoru V a zvolíme bod $O \in$ kterému budeme říkat *počátek*. Souřadnicový systém budeme značit $(O, B$

Souřadnice vektoru $\boldsymbol{u} \in V$ vzhledem k systému (O, B) jsou souřad vektoru $\boldsymbol{u}$ vzhledem k uspořádané bázi (B).

Souřadnice bodu $P \in \mathbf{X}$ vzhledem k systému (O, B) jsou souřadnice toru $P - O$ vzhledem k uspořádané bázi (B). Vektor $P - O$ se nazývá *radius tor bodu P*.

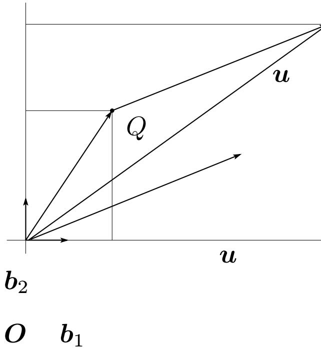
Dimenze afinního prostoru $(\mathbf{X}, V)$ je rovna dimenzi lineárního prostoru Typicky používáme afinní prostory dimenze 2 (rovina) nebo dimenze 3 (geometrické vnímání světa).

[esour-lin] Nechť $(\mathbf{X}, V)$ je afinní prostor, nechť dále (O, B) je jeho sou nicový systém. Nechť $\boldsymbol{u} \in V$, $\boldsymbol{v} \in V$ $\alpha \in \mathbf{R}$, $P \in \mathbf{X}$, $Q \in \mathbf{X}$. Symbolem značíme souřadnice bodu nebo vektoru vzhledem k (O, B). Platí

$$\begin{aligned} &(1)\ \mathcal{C}(\boldsymbol{u} + \boldsymbol{v}) = \mathcal{C}(\boldsymbol{u}) + \mathcal{C}(\boldsymbol{v}) \\ &(2)\ \mathcal{C}(\alpha \cdot \boldsymbol{u}) = \alpha \cdot \mathcal{C}(\boldsymbol{u}) \\ &(3)\ \mathcal{C}(Q + \boldsymbol{u}) = \mathcal{C}(Q) + \mathcal{C}(\boldsymbol{u}) \\ &(4)\ \mathcal{C}(P - Q) = \mathcal{C}(P) - \mathcal{C}(Q) \end{aligned}$$

(4) Vektor $P - Q$ je výsledkem operace „radiusvektor bodu P minus diusvektor bodu Q“. Další argumentace je stejná jako v důkazu (3).

[PQ] 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 meno $\boldsymbol{u}$, protože tyto úsečky jsou rovnoběžné, stejně velké a stejně orientov Považujeme je za reprezentanty stejného vektoru $\boldsymbol{u}$.

* [dhomosour] Nechť $(\mathbf{X}, V)$ je afinní prostor dimenze n a (O, B) je souřadnicový systém.

Homogenní souřadnice bodu $P \in \mathbf{X}$ jsou uspořádaná $(n+1)$-tice, kte prvních n složkách obsahuje souřadnice bodu P vzhledem k (O, B) a v posl složce obsahuje jedničku.

Homogenní souřadnice vektoru $\boldsymbol{u} \in V$ jsou uspořádaná $(n+1)$-tice, k v prvních n složkách obsahuje souřadnice vektoru $\boldsymbol{u}$ vzhledem k (O, B) poslední složce obsahuje nulu.

Upozornění: rozšířenou verzi definice homogenních souřadnic bodu p

Důkaz. V případě lineárních kombinací vektorů zůstává v poslední složce řadnic nula. Při součtu bodu s vektorem je v poslední složce souřadnic odeh výpočet $1 + 0 = 1$, tedy dostáváme homogenní souřadnice bodu. Při odečí bodů se v poslední složce souřadnic odečítají jedničky a vzniká nula, dostáv tedy homogenní souřadnice vektoru.

* [Ahomo] Nechť $(\mathbf{X}, V)$ je afinní prostor dimenze n a (O, B) jeho sou nicový systém. Říkáme, že *transformace* $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$ *má matici* $\mathbf{A} \in \mathbf{R}^{n+1}$ *v homogeních souřadnicích vzhledem k* (O, B), pokud pro každý bod P jsou homogenní souřadnice obrazu $\mathcal{A}(P)$ rovny sloupcovému vektoru $\mathbf{A} \cdot \boldsymbol{x}$, $\boldsymbol{x}$ jsou homogenní souřadnice bodu P. Jinak řečeno, pro každý bod $P \in \mathbf{X}$

$$\mathbf{A} \cdot \begin{pmatrix} \text{homogenní} \\ \text{souřadnice} \\ \text{bodu } P \\ \text{vzhledem} \\ \text{k } (O, B) \end{pmatrix} = \begin{pmatrix} \text{homogenní} \\ \text{souřadnice} \\ \text{bodu } \mathcal{A}(P) \\ \text{vzhledem} \\ \text{k } (O, B) \end{pmatrix}$$

Nechť transformace $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$ má matici $\mathbf{A}$. Jak musí taková ma vypadat? Je-li $\boldsymbol{x}$ vektor homogenních souřadnic bodu, pak musí $\mathbf{A} \cdot \boldsymbol{x}$ být vektor homogenních souřadnic bodu. Neboli jednička v poslední složce vek $\boldsymbol{x}$ musí zůstat zachována i po maticovém násobení. Z vlastností maticov náspobení vyplývá, že daný požadavek splňují všechny matice $\mathbf{A} \in \mathbf{R}^{n+1,}$ které je možné do bloků rozepsat následovně:

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}' & \boldsymbol{t} \\ \boldsymbol{o} & 1 \end{pmatrix}, \qquad (typA)$$

kde $\mathbf{A}' \in \mathbf{R}^{n,n}$ je libovolná matice, $\boldsymbol{t} \in \mathbf{R}^{n,1}$ je libovolný sloupcový vek $\boldsymbol{o} \in \mathbf{R}^{1,n}$ je nulový vektor a vpravo dole je jednička. Jinými slovy je to ma

Z maticového násobení snadno plyne, že součin dvou matic typu (??) je
tice typu (??). Tento součin je maticí odpovídajícího složeného zobrazení,
ukážeme ve větě ??.

V afinním prostoru dimenze 2 jsou matice transformací v homogen
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
f.

V afinním prostoru dimenze 3 jsou matice transformací v homogen
souřadnicích tvaru:

$$\begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \text{tj.} \quad \begin{pmatrix} x' \\ y' \\ z' \\ 1 \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \\ 1 \end{pmatrix} = \begin{pmatrix} ax + by \\ ex + fy \\ ix + jy \\ \end{pmatrix}$$

Transformace v 3D prostoru jsou tedy určeny maticemi s dvanácti param
a až l.

* [slozhomo] Nechť $(\mathbf{X}, V)$ je afinní prostor dimenze n a nechť $(O, B$
jeho souřadnicový systém. Nechť transformace $\mathcal{A} \colon \mathbf{X} \to \mathbf{X}$ má matici
homogenních souřadnicích vzhledem k (O, B) a transformace $\mathcal{B} \colon \mathbf{X} \to \mathbf{X}$
matici $\mathbf{B}$ v homogenních souřadnicích vzhledem k (O, B). Pak složené zobra
$\mathcal{B} \circ \mathcal{A}$ 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
toru vzhledem k bázi“ v důkazu používáme slova „homogenní souřadnice b
vzhledem k (O, B)“.

[elemhomo] Uvedeme matice elementárních transformací v afinním

Změna měřítka tansformuje vektory stejně jako body. Tento typ transforn
byl podrobně diskutován v příkladu ??.

Rotace o úhel α kolem počátku má matici

$$\begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{protože} \quad \begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} x\ \mathrm{c} \\ x\ \mathrm{s} \\ \end{pmatrix}$$

Rotace transformuje vektory stejně jako body. Matice tohoto typu transforn
byla odvozena v příkladu ??. Doplňujícím předpokladem pro tuto matic
souřadnicový systém s bází vektorů, které jsou na sebe kolmé a mají stej
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 tě
elementárních trnasformací. Složené zobrazení má podle věty ?? matici ro
součinu matic jednotlivých zobrazení.

V afinním prostoru dimenze 2 najdeme matici $\mathbf{A}$ v homogenních sou
nicích takové transformace, která otáčí vzor kolem bodu se souřadnicemi (
o úhel α. Tato transformace je složením tří transformací: nejprve posune
$(2, 3)$ do počátku, pak otočí obraz kolem počátku o úhel α a nakonec pos
počátek zpět do bodu $(2, 3)$. Matice transformace je součinem matic trans
mací, ze kterých je složena, přitom nejdříve aplikovaná transformace má s
matici nejvíce vpravo (viz větu ??).

V dalším textu ukážeme, že všechny transformace $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$, které m
matici v homogenních souřadnicích, jsou tzv. *afinní transformace* a dále d
žeme, že všechny afinní transformace mají matici v homogenních souřadnic

* [Atrans] Nechť $(\mathbf{X}, V)$ je afinní prostor. Transformace $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$ se
zývá *afinní transformace* (krátce *afinita*), pokud existuje lineární transform
$\mathcal{A}'\colon V \to V$ tak, že pro každý bod $P \in \mathbf{X}$ a pro každý vektor $\boldsymbol{u} \in V$ platí

$$\mathcal{A}(P + \boldsymbol{u}) = \mathcal{A}(P) + \mathcal{A}'(\boldsymbol{u}).$$

* [anabasi] Nechť $(\mathbf{X}, V)$ je afinní prostor dimenze n a $(O, B) = (O, \boldsymbol{b}_1, .$
je jeho souřadnicový systém. Pak afinní zobrazení $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$ je jednozna
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 k
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 hodn
$\mathcal{A}'(\boldsymbol{b}_i)$ pro všechny bázové vektory $\boldsymbol{b}_i$. Lineární zobrazení $\mathcal{A}'$ je podle věty
těmito hodnotami jednoznačně určeno. Hodnota zobrazení $\mathcal{A}$ v každém b
$P \in \mathbf{X}$ je pak jednoznačně určena ze vztahu

$$\mathcal{A}(P) = \mathcal{A}\big(O + (P - O)\big) = \mathcal{A}(O) + \mathcal{A}'(P - O).$$

[Ahomoa] Nechť $(\mathbf{X}, V)$ je afinní prostor dimenze n a (O, B) je jeho
řadnicový systém. Pak každá transformace $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$, která má matici
homogenních souřadnicích vzhledem k (O, B), je afinní transformace.

Důkaz. Nechť $\mathbf{A}$ je matice zobrazení $\mathcal{A}$ v homogenních souřadnicích. Pa

takže maticové násobení $\mathbf{A}\cdot\boldsymbol{x}$ transformuje také homogenní souřadnice vek
na homogenní souřadnice vektorů. K této transformaci homogenních souřa
vektorů existuje zpětně transformace vektorů samotných $\mathcal{A}'\colon V\to V$ takov
homogenní souřadnice obrazu $\mathcal{A}'(\boldsymbol{u})$ jsou rovny sloupcovému vektoru

$$\mathbf{A}\cdot\begin{pmatrix}\boldsymbol{c}^T\\0\end{pmatrix}.$$

Tato transformace $\mathcal{A}'\colon V\to V$ je zjevně lineární a má matici $\mathbf{A}'$ vzhlede
bázi (B).

Nyní stačí dokázat, že $\mathcal{A}(P+\boldsymbol{u})=\mathcal{A}(P)+\mathcal{A}'(\boldsymbol{u})$ pro všechny body P
a všechny vektory $\boldsymbol{u}\in V$. Tato rovnost platí, protože

$$\mathbf{A}\cdot\left(\begin{pmatrix}\boldsymbol{p}^T\\1\end{pmatrix}+\begin{pmatrix}\boldsymbol{c}^T\\0\end{pmatrix}\right)=\mathbf{A}\cdot\begin{pmatrix}\boldsymbol{p}^T\\1\end{pmatrix}+\mathbf{A}\cdot\begin{pmatrix}\boldsymbol{c}^T\\0\end{pmatrix}$$

* [zobhomo] Nechť $(\mathbf{X},V)$ je afinní prostor dimenze n se souřadnico
systémem (O,B). Pak každé afinní zobrazení $\mathcal{A}$ má matici $\mathbf{A}$ v homogen
souřadnicích vzhledem k (O,B).

Důkaz. Protože $\mathcal{A}$ je afinní, existuje lineární transformace $\mathcal{A}'\colon V\to V$
že $\mathcal{A}(P+\boldsymbol{u})=\mathcal{A}(P)+\mathcal{A}'(\boldsymbol{u})$ pro všechny body $P\in\mathbf{X}$ a všechny vek
$\boldsymbol{u}\in V$. Do matice $\mathbf{A}$ zapíšeme nejprve homogenní souřadnice obrazů bázov
vektorů $\mathcal{A}'(\boldsymbol{b}_i)$ a do posledního sloupce zapíšeme obraz $\mathcal{A}(O)$. Takto sesta
matice je zjevně typu (??). Označme $\mathcal{B}\colon\mathbf{X}\to\mathbf{X}$ transformaci, která má m
$\mathbf{A}$ v homogenních souřadnicích. Podle věty ?? je $\mathcal{B}$ afinní transformace. K
ukážeme, že $\mathcal{B}(O)=\mathcal{A}(O)$ a dále $\mathcal{B}(O+\boldsymbol{b}_i)=\mathcal{A}(O+\boldsymbol{b}_i)$ pro všechny bá
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 posl sloupce matice $\mathbf{A}$ s posledním, tedy obsahuje (podle pravidla sestavení tice) homogenní souřadnice obrazu $\mathcal{A}(O) + \mathcal{A}'(\boldsymbol{b}_i) = \mathcal{A}(O + \boldsymbol{b}_i)$. Z toho p $\mathcal{B}(O + \boldsymbol{b}_i) = \mathcal{A}(O + \boldsymbol{b}_i)$.

Nechť má afinní prostor $(\mathbf{X}, V)$ dimenzi n. Afinní transformace $\mathcal{A}\colon \mathbf{X}$ - je prostá právě tehdy, když je na.

Důkaz. Afinní transformace $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$ je prostá právě tehdy, když její při žená lineární transformace $\mathcal{A}'\colon V \to V$ je prostá, právě tehdy, když def $\mathcal{A}'$ právě tehdy, když hod $\mathcal{A}' = n$ (viz větu ??) právě tehdy, když $\mathcal{A}'$ je na V p tehdy, když $\mathcal{A}$ je na $\mathbf{X}$.

* Složení dvou afinních transformací je afinní transformace.

Důkaz. Ve větě ?? jsme ukázali, že složením dvou transformací, které svou matici v homogenních souřadnicích, je transfrormace, která má mat homogenních souřadnicích. Dále ve větách ?? a ?? jsme ukázali, že tranfsorn má matici v homogenních souřadnicích právě tehdy, když je afinní.

Inverzní transformace k prosté afinní transformaci je afinní.

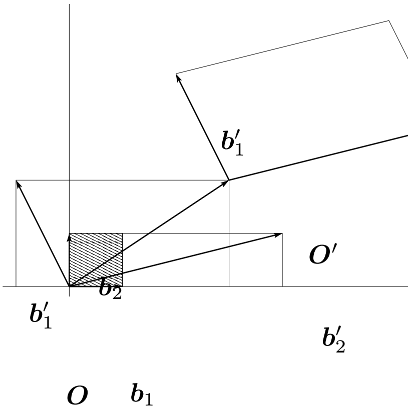
Důkaz. Má-li původní transformace matici $\mathbf{A}$ v homogenních souřadni pak inverzní transformace má matici $\mathbf{A}^{-1}$ v homogenních souřadnicích.

Prostá afinní transformace transformuje rovnoběžné přímky na rovnob přímky.

Důkaz. Přímka v afinním prostoru $(\mathbf{X}, V)$ je množina $p = \{P + t\boldsymbol{u};\ t \in \mathbf{R}\}$, $P \in \mathbf{X}$ je nějaký bod a $\boldsymbol{u} \in V$ je nenulový vektor. Vektoru $\boldsymbol{u}$ v tomto kont říkáme *směrový vektor přímky*. Dvě přímy jsou rovnoběžné nebo totožné, p jejich směrové vektory jsou lineárně závislé (tedy jeden je nenulovým násob druhého).

Nechť $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$ je prostá afinní transformace a označme $p = \{P + t\boldsymbol{u}$ $\mathbf{R}\}$ a $q = \{Q + t\boldsymbol{v};\ t \in \mathbf{R}\}$ dvě různé rovnoběžné přímky. Takže $\boldsymbol{u} = \alpha \boldsymbol{v}$. I [arovnobeznost] Předpokládejme nyní, že afinní zobrazení není prost tomto případě se přímky mohou zobrazit do bodu nebo dvě rovnoběžné pří se zobrazí do jedné přímky. Projděte si důkaz předchozí věty znova a rozmys si, že afinní zobrazení, které nemusí být prosté, nikdy nezobrazí rovnoběžk různoběžky.

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 požada na posunutí bodu O do O', je tím také určena transformace $\mathcal{A} : \mathbf{X} \to \mathbf{X}$. Ma této transformace má podle důkazu věty ?? homogenní souřadnice vektor a bodu O' v odpovídajících sloupcích. Aby se nám na obrázku souřadnice torů $\boldsymbol{b}_i'$ vzhledem k bázi (B) dobře hledaly, překreslili jsme jejich orientov úcečky také tak, aby začínaly v bodě O. Vidíme, že vektorů $\boldsymbol{b}'_1$, $\boldsymbol{b}'_2$ a bodu O':

$$\mathbf{A} = \begin{pmatrix} -1 & 4 & 3 \\ 2 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Dá se ukázat, že každá afinní transformace afinního prostoru dimenze
výsledkem skládání elementárních operací změny měřítka, otočení a posu
uvedených v příkladu ??. Důkaz tohoto tvrzení ponecháme až do kapitoly
nácté v příkladu ??.

[perspproj] V počítačové grafice se řeší otázka zobrazení 3D modelu
2D stínítko monitoru. Můžeme to udělat odstraněním například souřadni
ze tří původních souřadnic 3D modelu, tedy $(x, y, z) \to (x, y)$. Toto zobra
nazýváme ortografickou projekcí. Přirozenější ale je představit si oko p
rovatele (nebo kameru) jako centrum, do kterého se sbíhají všechny papr
odrážející se od pozorovaných objektů. Před pozorovatele postavíme stín
monitoru – průhlednou rovinu. Každý pozorvaný bod má svůj paprsek sm
jící do oka a průsečík tohoto paprsku s rovinou stínítka je obraz pozorovan
bodu při perspektivní projekci. Situace je znázorněná na obrázku. Zde je
pozorovatele umístěné do počátku souřadnic afinního prostoru a rovina stín
je kolmá na osu z a je umístěna ve vzdálenosti 1 od pozorovatele. Pozor
tel se dívá „nahoru“. Je docela pohodlné ležet na gauči a zírat vzhůru
této situace se bod 3D scény se souřadnicemi (x, y, z) zobrazí na stínítko
místa se souřadnicemi $(x/z, y/z, 1)$ a po zanedbání souřadnice z máme výsle
2D souřadnice $(x/z, y/z)$. Tuto perpektivní projekci tedy můžeme popsat
$(x, y, z) \to (x/z, y/z)$. Zjevně body se souřadnicemi $(x, y, 0)$ původní 3D s
nejsou vidět a do 2D scény se nezobrazují. Pravda, nejsou vidět ani bod
zády pozorovatele, tj. (x, y, z) pro $z < 0$. Pokud bychom je před projekcí n
stranili, pak by se nám při použití vzorce $(x, y, z) \to (x/z, y/z)$ také prom

můžeme pomocí maticového násobení postihnout i perspektivní projekci. třebujeme k tomu účelu ovšem rozšířit pojem homogenní souřadnice bod poslední souřadnici od této chvíle připustíme jakékoli nenulové číslo, ne n jedničku:

* [dhomo2] Nechť $(\mathbf{X}, V)$ je afinní prostor a (O, B) jeho souřadnicový tém. Nechť bod $P \in \mathbf{X}$ má vzhledem k (O, B) souřadnice $(x_1, x_2, \ldots, x_n)$. jakoukoli uspořádanou $(n+1)$-tici $(tx_1, tx_2, \ldots, tx_n, t)$ pro $t \neq 0$ nazýv *homogenní souřadnice bodu* P.

Homogenní souřadnice bodu nejsou určeny touto definicí jednoznačně. žeme použít následující geometrickou představu: všechny homogenní souřad stejného bodu P z afinního prostoru $(\mathbf{X}, V)$ dimenze n vyplní (až na počá přímku v prostoru $\mathbf{R}^{n+1}$ homogenních souřadnic. Tato přímka vždy proc počátkem prostoru $\mathbf{R}^{n+1}$. V prostoru homogenních souřadnic $\mathbf{R}^{n+1}$ si vytvo zobecněnou rovinu $\varrho = \{(x_1, x_2, \ldots, x_n, 1),\ x_i \in \mathbf{R}\}$. Bod P je v prostoru mogenních souřadnic reprezentován přímkou, která protíná rovinu ϱ v P (po zanedbání poslední souřadnice). Všechny objekty v $\mathbf{X}$ mají v pros homogenních souřadnic o jednu dimenzi více, než v $\mathbf{X}$ samotném. Napří přímka v $\mathbf{X}$ je rovinou v $\mathbf{R}^{n+1}$ procházející počátkem. Přitom průsečík roviny se zobecněnou rovinou ϱ dává původní přímku.

Pro popis perspektivní projekce 3D scény na 2D stínítko si vystač s afinním prostorem dimenze 3 a se čtyřmi homogenními souřadnicem vstupu a s afinním prostorem dimenze 2 a třemi homogenními souřadnic na výstupu. Popíšeme perspektivní projekci, která je ve skutečných souřa cích popsána vzorcem $(x, y, z) \to (x/z, y/z)$ a byla zmíněna v poznámce Nechť homogenní souřadnice vzoru v této projekci jsou $(x, y, z, 1)$. Homog souřadnice obrazu jsou třeba $(x/z, y/z, 1)$, ale stejný bod má též (v soula definicí ?? a při volbě $t = z$) homogenní souřadnice (x, y, z). Matice pers tivní projekce v homogenních souřadnicích tedy vypadá následovně:

Chceme-li zjistit skutečné souřadnice tohoto bodu, musíme najít jiné ho genní souřadnice stejného bodu, které mají v poslední složce jedničku. T $(x/z, y/z, 1)$. Skutečné 2D souřadnice tedy podle očekávání jsou $(x/z, y/z$

Afinní prostor sestává z množiny bodů $\mathbf{X}$ a z lineárního prostoru V / Je definována operace „bod plus vektor je bod", která splňuje axiomy (1 (3) /??/.

Souřadnice bodu P jsou souřadnice jeho radiusvektoru $P - O$. Souřad bodů i vektorů zachovávají potřebné operace /??/.

Homogenní souřadnice bodu jsou souřadnice bodu následované jedničk homogenní souřadnice vektoru jsou souřadnice vektoru následované nulou /

Transformace $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$ jsou afinní, právě když mají matici v homo ních souřadnicích /??, ??, ??, ??/. Skládání afinních transformací má v ho genních souřadnicích matici rovnou součinu matic jednotlivých transforma

Matice v homogenních souřadnicích má vždy v posledním řádku $(0, \ldots,$

Uvedli jsme si matice elementárních transformací: změna měřítka, ro a posunutí /??/. Skládáním elementárních transformací lze vytvořit libovol afinní transformaci.

Nechť $(\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n, O)$ je souřadnicový systém prostoru $(\mathbf{X}, V)$ Af transformace $\mathcal{A}\colon \mathbf{X} \to \mathbf{X}$ je jednoznačně určena svými obrazy bodu O a b $O + \boldsymbol{b}_i$ /??/. Matice této transformace v homogeních souřadnicích má ve slo cích homogenní souřadnice obrazů $\boldsymbol{b}_i$ následované sloupcem s homogenn souřadnicemi obrazu bodu O.

12. Vlastní číslo, vlastní vektor

Předpokládejme, že je dána lineární transformace $\mathcal{A}\colon \mathbf{R}^2 \to \mathbf{R}^2$, kterou svou matici $\mathbf{A} \in \mathbf{R}^{2,2}$. Je-li $\boldsymbol{u} \in \mathbf{R}^2$ nenulový vektor, pak množina $p = \{t\boldsymbol{u}$ $\mathbf{R}\}$ je (z geometrického pohledu) přímka, procházející počátkem. Nenulov vektoru $\boldsymbol{u}$ říkáme *směrový vektor přímky*. Transformace $\mathcal{A}$ zobrazuje pří procházející počátkem na přímky procházející počátkem. Pokusíme se n přímku procházející pořátkem, která se tranformací $\mathcal{A}$ zobrazí sama na seb

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 $\mathcal{A}$ 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 formul takto: najít nenulový vektor $\boldsymbol{u} \in \mathbf{R}^2$ a číslo $\lambda \in \mathbf{R}$ tak, aby $\mathbf{A}\cdot\boldsymbol{u} = \lambda\boldsymbol{u}$. Rov 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 n nenulové řešení $\boldsymbol{u}$ této homogenní soustavy (s parametrem $\lambda \in \mathbf{R}$), musí matice $\mathbf{A} - \lambda\mathbf{E}$ být singulární, neboli musí $\det(\mathbf{A} - \lambda\mathbf{E}) = 0$. Je-li dána ma $\mathbf{A} \in \mathbf{R}^2$, pak rovnice $\det(\mathbf{A} - \lambda\mathbf{E}) = 0$ je kvadratická rovnice v proměnn Tato rovnice může, ale nemusí mít reálné kořeny. Pokud má reálné kořeny a λ_2, pak lze najít nenulová řešení homogenních soustav $(\mathbf{A} - \lambda_1\mathbf{E})\cdot\boldsymbol{u} =$ $(\mathbf{A} - \lambda_2\mathbf{E})\cdot\boldsymbol{u} = \boldsymbol{o}$. Označíme-li tato řešení $\boldsymbol{u}_1$ a $\boldsymbol{u}_2$, pak jsme našli dvě pří $p_1 = \{t\boldsymbol{u}_1\}$ a $p_2 = \{t\boldsymbol{u}_2\}$, které se zobrazí na sebe. Uvedený postup ukázán následujících příkladech znovu a konkrétněji.

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:

Kořeny $\lambda = 2$ a $\lambda = 3$ postupně dosadíme do původní homogenní soustavy

$$\lambda = 2: \quad \begin{pmatrix} 5-2 & 2 \\ -3 & -2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \qquad \lambda = 3: \quad \begin{pmatrix} 5-3 & 2 \\ -3 & -3 \end{pmatrix} \cdot \begin{pmatrix} x \\ x \end{pmatrix}$$

Nenulové řešení první soustavy je například $(-2, 3)$ a nenulové řešení dr soustavy je $(-1, 1)$. Takže přímky $p_1 = \{t(-2, 3);\ t \in \mathbf{R}\}$ a $p_2 = \{t(-1, 1)$ $\mathbf{R}\}$ jsou hledané přímky, které se zobrazí na sebe.

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 do váme determinant:

$$\det \begin{pmatrix} 1-\lambda & 2 \\ -2 & 3-\lambda \end{pmatrix} = 0, \quad \text{tj.} \quad \lambda^2 - 4\lambda + 7 = 0, \quad \text{tato rovnice nemá v } \mathbf{R} \text{ ř}$$

V tomto případě neexistuje žádná přímka procházející počátkem, kterou daná lineární transformace ponechala beze změny.

Číslům λ v předchozích příkladech se říká *vlastní čísla matice* $\mathbf{A}$, n *vlastní čísla transformace* $\mathcal{A}$. Směrovým vektorům přímek, které transform ponechává beze změny, říkáme *vlastní vektory*. Přesnější definici těchto po zavedeme za chvíli.

Z uvedených příkladů plyne, že vlastní čísla matice $\mathbf{A}$ lze počítat kořeny polynomu $\det(\mathbf{A} - \lambda\mathbf{E})$. Tyto kořeny ovšem nemusejí být vždy re Abychom měli zaručenu vždy existenci vlastního čísla, budeme muset při tit i komplexní vlastní čísla a komplexní vlastní vektory. V této kapitole bude užitečné pracovat s lineárními prostory nad komplexními čísly (vi

V modelových příkladech se pokusíme komplexním číslům vyhnout.

* [dvl] Nechť L je lineární prostor konečné dimenze nad $\mathbf{C}$ a nechť $\mathcal{A}\colon$ L je lineární transformace. Číslo $\lambda \in \mathbf{C}$ se nazývá *vlastním číslem trans-mace $\mathcal{A}$*, pokud existuje vektor $\boldsymbol{x} \in L$, $\boldsymbol{x} \neq \boldsymbol{o}$ takový, že $\mathcal{A}(\boldsymbol{x}) = \lambda\, \boldsymbol{x}$. Ve $\boldsymbol{x}$, který splňuje uvedenou rovnost, se nazývá *vlastní vektor transformac příslušný vlastnímu číslu λ*.

Pokud existuje vlastní číslo transformace $\mathcal{A}$, pak mu přísluší více vl-ních vektorů. Přidáme-li k těmto vektorům vektor nulový, dostáváme line podprostor prostoru L. Skutečně, pokud $\boldsymbol{x}$, $\boldsymbol{y}$ splňují $\mathcal{A}(\boldsymbol{x}) = \lambda\, \boldsymbol{x}$, $\mathcal{A}(\boldsymbol{y}) =$ pak

$$\mathcal{A}(\boldsymbol{x}+\boldsymbol{y}) = \mathcal{A}(\boldsymbol{x})+\mathcal{A}(\boldsymbol{y}) = \lambda\, \boldsymbol{x}+\lambda\, \boldsymbol{y} = \lambda\,(\boldsymbol{x}+\boldsymbol{y}), \qquad \mathcal{A}(\alpha\, \boldsymbol{x}) = \alpha\, \mathcal{A}(\boldsymbol{x}) = \alpha\lambda$$

Pojem vlastní číslo definujeme nejenom pro lineární transformace, ale něž pro čtvercové matice. Záhy zjistíme, že mezi vlastním číslem transforn a její matice je úzká souvislost.

* [dvA] Nechť $\mathbf{A}$ je čtvercová matice typu (n, n) reálných nebo komplex čísel. Číslo $\lambda \in \mathbf{C}$ se nazývá *vlastním číslem matice* $\mathbf{A}$, pokud existuje ve $\boldsymbol{x} \in \mathbf{C}^{n,1}$, $\boldsymbol{x} \neq \boldsymbol{o}$, takový, že $\mathbf{A} \cdot \boldsymbol{x} = \lambda\, \boldsymbol{x}$. Vektor $\boldsymbol{x}$, který splňuje uvede rovnost, se nazývá *vlastní vektor matice* $\mathbf{A}$ *příslušný vlastnímu číslu λ*.

[vlavlA] Nechť $\mathcal{A}\colon L \to L$ je lineární transformace a $\mathbf{A}$ je jeho ma vzhledem k nějaké bázi (B). Pak λ je vlastním číslem transformace $\mathcal{A}$ p tehdy, když je vlastním číslem matice $\mathbf{A}$. Navíc $\boldsymbol{x}$ je vlastní vektor transforn $\mathcal{A}$ příslušný λ právě tehdy, když souřadnice vektoru $\boldsymbol{x}$ vzhledem k bázi (B) t 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). Ta $\mathcal{A}(\boldsymbol{x}) = \lambda\, \boldsymbol{x}$ právě tehdy, když $\mathbf{A} \cdot \boldsymbol{u} = \lambda\, \boldsymbol{u}$.

Množina všech vlastních čísel lineární transformace nebo matice se na zřejmé, že λ bude vlastním číslem matice $\mathbf{A}$ právě tehdy, když homog soustava s maticí $\mathbf{A} - \lambda\,\mathbf{E}$ bude mít nenulové řešení. Tímto řešením pak b vlastní vektor příslušný vlastnímu číslu λ. Aby tato soustava měla nenu řešení, musí její matice být singulární, tj. musí $\det(\mathbf{A} - \lambda\,\mathbf{E}) = 0$. Tím m odvozen vzorec na výpočet vlastních čísel. Uvědomíme si ještě, že $\det(\mathbf{A} -$ je polynom v proměnné λ. Tento polynom se nazývá *charakteristický poly* matice $\mathbf{A}$. Jeho stupeň je stejný, jako počet řádků matice $\mathbf{A}$. Označme toto n. Abychom tedy našli všechna vlastní čísla dané matice, stačí najít všec kořeny charakteristického polynomu této matice. Podle základní věty alg těchto kořenů (včetně jejich násobnosti) je n. Každá matice má tedy n vlast čísel (obecně ne vzájmeně různých). Každá lineární transformace $\mathcal{A}\colon L$ má tolik vlastních čísel, kolik je dimeze L.

[chpolynom] Nechť $\mathbf{A}$ je čtvercová matice. Polynom $\det(\mathbf{A}-\lambda\,\mathbf{E})$ nazýv *charakteristický polynom matice* $\mathbf{A}$ a rovnost $\det(\mathbf{A} - \lambda\,\mathbf{E}) = 0$ charakteri kou rovnicí. Je-li λ k-násobným kořenem charakteristické rovnice, říkáme, je *k-násobným vlastním číslem*.

[3vvektory] Uvedeme ještě celý postup odvození výpočtu vlastních matice (viz předchozí poznámku) znovu na konkrétním numerickém příkl protože odvození může pro někoho být na konkrétním příkladě názornější. deme 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 splněna maticová rovnost

$$\begin{pmatrix} 5 & -2 & 2 \\ -1 & 4 & -1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \lambda \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

Potřebujeme, aby uvedená homogenní soustava se čtvercovou maticí měla
nulové řešení. Matice soustavy tedy musí být singulární, tj. musí mít nu
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 nebud
opakovat, ale začneme rovnou od rovnice $\det(\mathbf{A}-\lambda\mathbf{E}) = 0$.

$$\det(\mathbf{A}-\lambda\mathbf{E}) = (5-\lambda)(4-\lambda)(-1-\lambda)-16-\big(-8(4-\lambda)-4(5-\lambda)+2(-1-\lambda)\big) =$$

takže vlastní čísla jsou $\lambda = 3$ a $\lambda = 2$. Najdeme ještě vlastní vektory. Nej
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 $\{(1,1,0), (-1$
Toto jsou dva lineárně nezávislé vlastní vektory, které přísluší vlastnímu čísl
Všechny vlastní vektory příslušející vlastnímu číslu 3 tvoří lineární obal
báze, ovšem bez nulového vektoru. Nyní najdeme vlastní vektory, které přís
vlastnímu číslu 2:

$$\begin{pmatrix} 5-2 & -2 & 2 \\ -1 & 4-2 & -1 \\ -4 & 4 & -1-2 \end{pmatrix} = \begin{pmatrix} 3 & -2 & 2 \\ -1 & 2 & -1 \\ -4 & 4 & -3 \end{pmatrix} \sim \begin{pmatrix} -1 & 2 & -1 \\ 0 & 4 & -1 \\ 0 & -4 & 1 \end{pmatrix} \sim \begin{pmatrix} -1 \\ 0 \end{pmatrix}$$

[2vvektory] Následující příklad ukazuje, že nemusí existovat tolik linea nezávislých vlastních vektorů, kolik řádků má matice. Budeme hledat vla 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 příkla Nyní vypočítáme vlastní vektory:

$$\lambda = 3: \quad \begin{pmatrix} 2-3 & 4 & -3 \\ -1 & 10-3 & -6 \\ -1 & 8 & -4-3 \end{pmatrix} = \begin{pmatrix} -1 & 4 & -3 \\ -1 & 7 & -6 \\ -1 & 8 & -7 \end{pmatrix} \sim \begin{pmatrix} -1 & 4 & -3 \\ 0 & 3 & -3 \\ 0 & 4 & -4 \end{pmatrix} \sim$$

$$\lambda = 2: \quad \begin{pmatrix} 2-2 & 4 & -3 \\ -1 & 10-2 & -6 \\ -1 & 8 & -4-2 \end{pmatrix} = \begin{pmatrix} 0 & 4 & -3 \\ -1 & 8 & -6 \\ -1 & 8 & -6 \end{pmatrix} \sim \begin{pmatrix} -1 & 8 & -6 \\ 0 & 4 & -3 \end{pmatrix}$$

Na rozdíl od předchozího příkladu vícenásobnému vlastnímu číslu 3 přísluš jeden lineárně nezávislý vlastní vektor. Tato matice má tedy dohromady dva lineárně nezávislé vlastní vektory: $(1,1,1), (0,3,4)$, které po řadě přísl vlastním číslům 3 a 2.

matice vzhledem k bázi (B) a $\mathbf{B}$ je její matice vzhledem k bázi (B'). 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 vět (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 $\mathbf{P}_{B'}$ $(\mathbf{P}_{B \to B'})^{-1} = \mathbf{P}^{-1}$ (viz větu ??), dostáváme $\mathcal{M}_{B'B'}(\mathcal{A}) = \mathbf{P}^{-1} \cdot \mathcal{M}_{B,B}(\mathcal{A})$ neboli $\mathbf{B} = \mathbf{P}^{-1} \cdot \mathbf{A} \cdot \mathbf{P}$.

* [dpodobnost] Matice $\mathbf{A}$ je *podobná* matici $\mathbf{B}$, pokud existuje regul matice $\mathbf{P}$ taková, že platí $\mathbf{B} = \mathbf{P}^{-1} \cdot \mathbf{A} \cdot \mathbf{P}$.

Je-li $\mathbf{A}$ podobná $\mathbf{B}$, pak je i $\mathbf{B}$ podobná $\mathbf{A}$, protože místo matice $\mathbf{P}$ můž použít matici $\mathbf{P}^{-1}$. Stačí tedy říkat, že matice jsou si vzájemně podobné. $\mathbf{A}$ podobná $\mathbf{B}$ a $\mathbf{B}$ podobná $\mathbf{C}$, pak je $\mathbf{A}$ podobná $\mathbf{C}$, protože součin regulár matic je matice regulární a protože $(\mathbf{PQ})^{-1} = \mathbf{Q}^{-1}\mathbf{P}^{-1}$. Matice je podo sama sobě, protože $\mathbf{E}$ je regulární.

Protože podobné matice jsou matice stejné lineární transformace, jen v dem k případně různým bázím, mají samozřejmě všechny vzájemně podo matice stejná vlastní čísla. V následující větě ukážeme, že mají i stejný cha teristický polynom.

* [vlcisloPAP] Podobné matice mají stejný charakteristický polynom.

Důkaz. Nechť $\mathbf{P}$ je regulární. Matice $\mathbf{P}^{-1}\mathbf{AP}$ je podobná matici $\mathbf{A}$. Vypočt její charakteristický polynom:

$$\det(\mathbf{P}^{-1}\mathbf{AP} - \lambda\,\mathbf{E}) = \det(\mathbf{P}^{-1}\mathbf{AP} - \lambda\,\mathbf{P}^{-1}\mathbf{EP}) = \det(\mathbf{P}^{-1}\mathbf{AP} - \mathbf{P}^{-1}\lambda\,\mathbf{E}$$
$$= \det(\mathbf{P}^{-1}\,(\mathbf{A} - \lambda\,\mathbf{E})\,\mathbf{P}) = \det \mathbf{P}^{-1}\,\det(\mathbf{A} - \lambda\,\mathbf{E})\,\det$$

protože $\det \mathbf{P}^{-1} \det \mathbf{P} = 1$.

Matice z příkladů ?? a ?? mají sice stejný charakteristický polynom. za chvíli ukážeme, že si nejsou podobné. Tvrzení věty ?? tedy nelze obráti má charakteristický polynom $(\lambda_1 - \lambda)\,(\lambda_2 - \lambda) \cdots (\lambda_n - \lambda)$, protože determin diagonální matice $\mathbf{D} - \lambda\,\mathbf{E}$ je roven součinu prvků na diagonále. Vlastní matice $\mathbf{D}$ tedy jsou $\lambda_1, \lambda_2, \ldots, \lambda_n$.

Vlastní vektor matice $\mathbf{D}$ příslušný vlastnímu číslu λ_i je vektor obsa jící samé nuly s výjimkou i-té složky, ve které je nějaké nenulové číslo, t jednička.

Matici $\mathbf{D}$ z tohoto příkladu budeme značit $\mathbf{D} = \mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$. ušetříme papír.

[PDAP] Nechť $\mathbf{A}$ je čtvercová matice typu (n, n). Sestavme libovolná k plexní čísla $\lambda_1, \ldots, \lambda_n$ do diagonální matice $\mathbf{D} = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ a libov nenulové vektory $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ z $\mathbf{C}^n$ zapišme do sloupců matice $\mathbf{P}$, tj. $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$. Pak platí: čísla $\lambda_1, \ldots, \lambda_n$ jsou vlastními čísly matice $\mathbf{A}$ a $\boldsymbol{x}_1, \ldots$ jsou jejich odpovídající vlastní vektory právě tehdy, když je splněna rovn $\mathbf{PD} = \mathbf{AP}$.

Důkaz. Rozepišme maticové násobení: $\mathbf{PD} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) \cdot \mathrm{diag}(\lambda_1, \ldots, \lambda$ $(\lambda_1\,\boldsymbol{x}_1, \ldots, \lambda_n\,\boldsymbol{x}_n)$. Dále je $\mathbf{AP} = \mathbf{A}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) = (\mathbf{A}\boldsymbol{x}_1, \ldots, \mathbf{A}\boldsymbol{x}_1)$. M tedy obě strany zkoumané rovnosti $\mathbf{PD} = \mathbf{AP}$ rozepsány do sloupců. Vid že rovnost v i-tém sloupci $\lambda_i\,\boldsymbol{x}_i = \mathbf{A}\boldsymbol{x}_i$ platí právě tehdy, když λ_i je vla číslo matice $\mathbf{A}$ a $\boldsymbol{x}_i$ je příslušný vlastní vektor.

[AjeD] Nechť má čtvercová matice $\mathbf{A}$ s n řádky n lineárně nezávis vlastních vektorů (každý z nich přísluší nějakému vlastnímu číslu matice). je matice $\mathbf{A}$ podobná diagonální matici.

Důkaz. Sestavíme diagonální matici $\mathbf{D}$ z vlastních čísel příslušných vlast vektorům $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$. Dále použijeme předchozí větu. Protože matice $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ obsahuje podle předpokladu věty lineárně nezávislé sloupce $\mathbf{P}$ regulární, takže je možné vztah $\mathbf{PD} = \mathbf{AP}$ vynásobit zprava maticí Dostáváme $\mathbf{A} = \mathbf{PDP}^{-1}$, takže matice $\mathbf{A}$ je podobná matici $\mathbf{D}$.

Matice z příkladu ?? má tři řádky a tři lineárně nezávislé vlastní vekt
Jsou tedy splněny předpoklady věty ?? a matice je podobná diagonální ma
Věta ?? nám dává návod, jak najít matici $\mathbf{P}$ a diagonální matici. Sestav
vlastní vektory $(1,1,0),(-1,0,1),(-2,1,4)$ do sloupců a dostáváme matic
Sestavíme v odpovídajícím pořadí vlastní čísla do diagonální matice, a do
váme matici $\mathbf{D}$, pro kterou platí $\mathbf{A} = \mathbf{PDP}^{-1}$. Konkrétně:

$$\mathbf{A} = \begin{pmatrix} 5 & -2 & 2 \\ -1 & 4 & -1 \\ -4 & 4 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 & -2 \\ 1 & 0 & 1 \\ 0 & 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & -2 \\ 1 & 0 & 1 \\ 0 & 1 & 4 \end{pmatrix}^{-1}$$

Matice z příkladu ?? nemá tolik lineárně nezávislých vlastních vekt
jako je počet jejích řádků. To znamená, že není podobná diagonální ma
(kdyby byla, pak dostaneme spor s větou ??. Protože matice z příkladu ?
podobná diagonální matici, zatímco matice z příkladu ?? není, nejsou si
matice ani vzájemně podobné.

[vlastnijsouLN] Vlastní vektory, které příslušejí vzájemně různým vlast
číslům, jsou lineárně nezávislé.

Důkaz. Jeden vlastní vektor je samozřejmě lineárně nezávislý, protože je p
definice nenulový. Dále postupujeme indukcí. Přepokládáme, že matice $\mathbf{A}$
lineárně nezávislé vlastní vektory $\boldsymbol{x}_1, \ldots \boldsymbol{x}_k$ příslušející různým vlastním
lům $\lambda_1, \ldots, \lambda_k$ a přidáme do této skupiny vlastní vektor $\boldsymbol{x}_{k+1}$ příslušející za
nepoužitému vlastnímu číslu λ_{k+1}. Předpokládáme rovnost $\sum_{i=1}^{k+1} \alpha_i \boldsymbol{x}_i =$
ukážeme, že všechny koeficienty α_i musejí být nulové. Tím dokážeme line
nezávislost. Vektory v uvedené rovnosti píšeme do sloupců a rovnost vyn
bíme zleva maticí $\mathbf{A} - \lambda_{k+1}\mathbf{E}$. Dostáváme:

$\alpha_i = 0$ pro $i \in \{1, \ldots, k\}$. Dosadíme-li tento poznatek do výchozího tvaru nosti, 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 $\boldsymbol{x}_{k+}$ vlastní vektor a tudíž nenulový, musí $\alpha_{k+1} = 0$.

[zarukapodobnosti] Nechť $\mathbf{A}$ je typu (n, n) a nechť jsou všechna vla čísla matice $\mathbf{A}$ jednonásobná. To znamená, že existuje n různých vlast čísel. Pak podle předchozí věty jim příslušející vlastní vektory jsou linea nezávislé. Podle věty ?? je tedy matice $\mathbf{A}$ podobná diagonální matici.

Má-li matice $\mathbf{A}$ vícenásobná vlastní čísla, pak se může stát, že je podo s diagonální maticí. Záleží na tom, zda se povede najít n lineárně nezávis vlastních vektorů. Vzhledem k tomu, že vlastní vektory leží v nulových pro rech matic $\mathbf{A} - \lambda\mathbf{E}$ (kde λ je vlastní číslo), půjde o to, jakou mají tyto pros dimenzi. Odpověď na to dávají následující věty.

Jestliže $\mathbf{A}$ a $\mathbf{B}$ jsou podobné matice, pak $\dim \mathrm{Null}(\mathbf{A} - \lambda\mathbf{E}) = \dim \mathrm{Null}($ $\lambda\mathbf{E})$.

Důkaz. Protože $\dim \mathrm{Null}(\mathbf{A} - \lambda\mathbf{E}) = n - \mathrm{hod}(\mathbf{A} - \lambda\mathbf{E})$, kde n je počet řá matice $\mathbf{A}$, stačí dokázat, že $\mathrm{hod}(\mathbf{A} - \lambda\mathbf{E}) = \mathrm{hod}(\mathbf{B} - \lambda\mathbf{E})$. Z věty ?? víme platí:

$$\mathrm{hod}(\mathbf{B} - \lambda\mathbf{E}) = \mathrm{hod}(\mathbf{P}^{-1}\mathbf{A}\mathbf{P} - \lambda\mathbf{P}^{-1}\mathbf{E}\mathbf{P}) = \mathrm{hod}(\mathbf{P}^{-1}(\mathbf{A} - \lambda\mathbf{E})\mathbf{P}) = \mathrm{hod}(\mathbf{A} -$$

[nullgek] Nechť λ_i je k-násobné vlastní číslo matice $\mathbf{A}$ a nechť d je dime nulového prostoru matice $\mathbf{A} - \lambda_i\mathbf{E}$. Pak $d \le k$.

Důkaz. V nulovém prostoru matice $\mathbf{A} - \lambda_i\mathbf{E}$ můžeme najít bázi, která má d torů: $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_d$ a doplníme ji na bázi prostoru $\mathbf{C}^n$: $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_d,$ Nechť $\mathcal{A}\colon \mathbf{C}^n \to \mathbf{C}^n$ je transformace definována vzorcem $\mathcal{A}(\boldsymbol{x}) = \mathbf{A}\boldsymbol{x}$ a nech je matice této transformace vzhledem k bázi (B). Je zřejmé, že matice $\mathbf{A}$ jsou si vzájemně podobné, protože jsou to matice stejné lineární transform Zvolme $\boldsymbol{b}_j$ z báze (B) pro $j \le d$. Souřadnice tohoto vektoru vzhledem k

takže λ_i je aspoň d-násobným kořenem charakteristického polynomu matic
tj. podle věty ?? je aspoň d-násobným kořenem charakteristického polyn
matice $\mathbf{A}$.

[N1cupN2] Nechť λ je vlastní číslo matice $\mathbf{A}$. Nechť N_1 je lineárně nezáv
množina vlastních vektorů, které nepřislušejí vlastnímu číslu λ a dále N
lineárně nezávislá množina vlastních vektorů, které příslušejí vlastnímu č
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 $N_2 = \{\boldsymbol{x}_{k+1}, \ldots, \boldsymbol{x}_m\}$. Line
nezávislost množiny vektorů $N_1 \cup N_2 = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m\}$ se ověří stejně
v důkazu věty ??. Lineární kombinaci těchto vektorů, kterou položíme ro
nulovému vektoru, násobíme zleva maticí $\mathbf{A} - \lambda\mathbf{E}$. Tím zjistíme, že koeficien
vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k$ musejí být nulové. Konečně kvůli tomu, že N_2 je line
nezávislá, dostáváme nulové koeficienty i u vektorů $\boldsymbol{x}_{k+1}, \ldots, \boldsymbol{x}_m$.

* Matice $\mathbf{A}$ je podobná s diagonální maticí právě tehdy, když pro ka
vlastní číslo λ_i násobnosti k_i platí $\dim \operatorname{Null}(\mathbf{A} - \lambda_i\mathbf{E}) = k_i$.

Důkaz. Nechť $\mathbf{A}$ typu (n, n) je podobná s diagonální maticí. Pak $\mathbf{P}$ ve vz
$\mathbf{AP} = \mathbf{PD}$ musí být regulární. V matici $\mathbf{P}$ jsou ve sloupcích vlastní vekt
takže musí existovat n lineárně nezávislých vlastních vektorů. Podle věty
můžeme z každého nulového prostoru matice $\mathbf{A} - \lambda_i\mathbf{E}$ vybrat maximáln
lineárně nezávislých vektorů. Jinde se vlastní vektory nenalézají. Abych
získali n lineárně nezávislých vlastních vektorů, je třeba z každého nulov
prostoru matice $\mathbf{A} - \lambda_i\mathbf{E}$ vzít právě k_i lineárně nezávislých vektorů, ta
$\dim \operatorname{Null}(\mathbf{A} - \lambda_i\mathbf{E}) = k_i$.

Nechť obráceně $\dim \operatorname{Null}(\mathbf{A} - \lambda_i\mathbf{E}) = k_i$. Z každého nulového prostoru
bereme k_i lineárně nezávislých vektorů. Množina všech takto vybraných
torů je podle věty ?? lineárně nezávislá, takže jimi sestavená matice $\mathbf{P}$ je r

vlastní vektor a tento pojem použít k vybudování regulární matice **P**, k převádí matici **A** na Jordanův kanonický tvar. Všechny tyto pojmy vyža hlubší studium a přesahují bohužel rámec tohoto úvodního textu. Pro studium lze doporučit [16].

Věty ?? a ?? se dají formulovat z úhlu pohledu lineární transformace:

[vvlzob] Nechť $\mathcal{A}\colon L \to L$ je lineární transformace, $\dim L = n$. Trans mace $\mathcal{A}$ má n lineárně nezávislých vlastních vektorů právě tehdy, když exis báze (B) prostoru L taková, že $\mathcal{A}$ má vzhledem k této bázi diagonální m **D**. Přitom na diagonále matice **D** jsou vlastní čísla transformace $\mathcal{A}$ a (B) obsahuje vlastní vektory příslušné vlastním číslům v matici **D** ve stej pořadí.

Důkaz. Zvolme nějakou výchozí bázi (V) prostoru L. Označme symbole matici transformace $\mathcal{A}$ vzhledem k bázi (V). Existence báze (B) takové matice transformace $\mathcal{A}$ vzhledem k ní je **D**, je ekvivalentní s platností vz $\mathbf{A} = \mathbf{PDP}^{-1}$, kde **P** je matice přechodu od (V) k (B). Dále při důkazu zení „právě tehdy když“ použijeme v jednom směru větu ??. V druhém sn použijeme větu ?? a skutečnost, že matice přechodu **P** obsahuje ve sloup souřadnice báze (B) vzhledem k bázi (V).

Při práci s lineární transformací se někdy hodí zvolit takovou bázi, ve k je matice této transformace „co nejbližší“ matici diagonální. Právě vyslov věta říká, že za jistých okolností lze zvolit bázi, vzhledem ke které je ma transformace přímo diagonální. Pak můžeme na danou transformaci poh jen jako na transformaci změny měřítka (λ_1 krát první souřadnice, λ_2 druhá souřadnice, atd. až λ_n krát poslední souřadnice).

Nechť dimenze L je rovna n a vraťme se k představě vlastních vektorů směrových vektorů přímek, které lineární transformace nechává beze změny motivační příklady v úvodu této kapitoly). Povede-li se najít n různých přím

Vlastní čísla počítáme jako kořeny chrakteristického polynomu det($\lambda\mathbf{E}$) /??/.

Dvě matice stejné transformace vzhledem k různým bázím se nazý podobné /??/. Mají stejný charakteristický polynom /??/.

Podobnost s diagonální maticí je zaručena pro matice se vzájemně různ vlastními čísly /??/. Ovšem i některé matice s násobnými vlastními čísly podobné s diagonální, ale ne všechny.

Je-li $\mathbf{D}$ diagonální matice, se kterou je podobná matice $\mathbf{A}$, pak $\mathbf{D}$ o huje vlastní čísla matice $\mathbf{A}$ a sestavíme-li do sloupců matice $\mathbf{P}$ vlastní vek odpovídající vlastním číslům $\mathbf{A}$, pak $\mathbf{A} = \mathbf{P}\mathbf{D}\mathbf{P}^{-1}$.

13. Lineární prostory se skalárním součinem

Lineární prostor je libovolná množina, na které je definováno sčítá
násobení konstantou tak, aby byly splněny vlastnosti (1) až (7) z definice
Pokud na takové množině navíc definujeme násobení prvků *mezi sebou* tak
výsledek násobení je reálné číslo a násobení splňuje níže uvedené vlastnost
až (4), definovali jsme na lineárním prostoru skalární součin. Ten nám um
pracovat s novými vlastnostmi prvků lineárního prostoru, jako je jejich veli
a úhel mezi dvěma prvky.

* [dlpss] Nechť L je lineární prostor. Operaci $\cdot : L \times L \to \mathbf{R}$ nazveme
lárním součinem, pokud splňuje $\forall \boldsymbol{x} \in L$, $\forall \boldsymbol{y} \in L$, $\forall \boldsymbol{z} \in L$, $\forall \alpha \in \mathbf{R}$ násled
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, nazývám
neárním prostorem se skalárním součinem.

Je třeba rozlišovat mezi podobně znějícími pojmy „skalární násobek“ a
lární součin“. Skalární násobek $\cdot : \mathbf{R} \times L \to L$ je násobek vektoru reálným
lem, který je definován v každém lineárním prostoru. Na druhé straně skal
součin $\cdot : L \times L \to \mathbf{R}$ je součin vektorů mezi sebou.

Upozorňujeme, že stejně jako v definici lineárního prostoru ??, jsou
vlastnostech (1) až (4) definice skalárního součinu používány symboly „+“ a
v různých významech podle toho, jakého typu jsou jejich operandy. Nepří

Dále připomínáme, že budeme symbol „·“ jako dosud často vynechá takže místo $\boldsymbol{x} \cdot \boldsymbol{y}$ budeme stručně psát $\boldsymbol{xy}$.

[complss] Všimneme si, že jsme v definici ?? lineárního prostoru defino tento prostor „nad reálnými čísly“, protože jsme definovali násobek vek *reálným číslem*. Nic nám ale nebránilo zcela stejně definovat násobek vek komplexním číslem. Až dosud jsme mohli nahradit slovo „reálné číslo“ slo „komplexní číslo“ a naše teorie by zůstala platná. Všechny předchozí věty nadále platily.

Kdybychom ale chtěli definovat skalární součin jako komplexní číslo, mu bychom upravit vlastnost (1) definice ?? takto:

$$(1) \quad \boldsymbol{xy} = \overline{\boldsymbol{yx}},$$

kde pruh nad komplexním číslem $\boldsymbol{yx}$ značí komplexně sdružené číslo. Něk tvrzení se tedy budou v případě komplexního skalárního součinu nepatrn šit od tvrzení, která níže dokážeme. Protože se většina čtenářů tohoto te nachází zatím v prvním semestru a nemá za sebou analýzu komplexních sel, zjednodušíme si život tím, že zůstaneme u reálných čísel. Pro odvo důležitých vlastností lineárních prostorů se skalárním součinem nám to b stačit. Zájemce o důsledky definice komplexního skalárního součinu odkáž například na učebnici [5].

[nulaxx] Nechť L je lineární prostor se skalárním součinem, $\boldsymbol{o}$ je jeho nu vektor. Pak pro všechna $\boldsymbol{x} \in L$, $\boldsymbol{y} \in L$ a $\boldsymbol{z} \in L$ platí: (1) $\boldsymbol{x} \cdot \boldsymbol{o} = \boldsymbol{o} \cdot \boldsymbol{x} = 0$ $\boldsymbol{z} \cdot (\boldsymbol{x} + \boldsymbol{y}) = \boldsymbol{zx} + \boldsymbol{zy}$.

Důkaz. První vlastnost plyne z vlastnosti (7) definice lineárního prostor 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 vlastnost vlastnosti (1) až (4):

$$
\begin{aligned}
&(1)\quad \boldsymbol{x}\cdot\boldsymbol{y} = x_1y_1 + x_2y_2 + \cdots + x_ny_n = y_1x_1 + y_2x_2 + \cdots + y_nx_n = \boldsymbol{y}\cdot\boldsymbol{x}\\
&(2)\quad (\boldsymbol{x}+\boldsymbol{y})\cdot\boldsymbol{z} = (x_1+y_1)\,z_1 + (x_2+y_2)\,z_2 + \cdots + (x_n+y_n)\,z_n =\\
&\qquad\qquad = x_1z_1 + x_2z_2 + \cdots + x_nz_n + y_1z_1 + y_2z_2 + \cdots + y_nz_n = \boldsymbol{x}\cdot\\
&(3)\quad (\alpha\cdot\boldsymbol{x})\cdot\boldsymbol{y} = \alpha x_1y_1 + \alpha x_2y_2 + \cdots + \alpha x_ny_n = \alpha\,(x_1y_1 + x_2y_2 + \cdots +\\
&(4)\quad \boldsymbol{x}\cdot\boldsymbol{x} = x_1^2 + x_2^2 + \cdots + x_n^2 \geq 0.
\end{aligned}
$$

Vidíme, že z $x_1^2 + x_2^2 + \cdots + x_n^2 = 0$ plyne $x_1 = x_2 = \cdots = x_n = 0$, takž splněna i druhá část vlastnosti (4).

Skalární součin na $\mathbf{R}^n$ definovaný vzorcem (??) nazýváme *standard skalárním součinem*. Následující příklady ukazují, že existují i jiné skal součiny na $\mathbf{R}^n$.

[nssnaR2] Definujme součin na $\mathbf{R}^2$ takto

$$(x_1, x_2)\cdot(y_1, y_2) = x_1y_1 + 6x_2y_2 + 2x_1y_2 + 2x_2y_1.$$

Ukážeme, že takto definovaný součin je skalárním součinem na $\mathbf{R}^2$.

Ověříme vlastnosti (1) až (4) definice ??

$$
\begin{aligned}
&(1)\quad (x_1, x_2)\cdot(y_1, y_2) = x_1y_1 + 6x_2y_2 + 2x_1y_2 + 2x_2y_1 =\\
&\qquad\qquad = y_1x_1 + 6y_2x_2 + 2y_1x_2 + 2y_2x_1 = (y_1, y_2)\cdot(x_1, x_2),\\
&(2)\quad \big((x_1, x_2) + (y_1, y_2)\big)\cdot(z_1, z_2) = (x_1+y_1)\,z_1 + 6(x_2+y_2)\,z_2 + 2(x_1 +\\
&\qquad\qquad = x_1z_1 + 6x_2z_2 + 2x_1z_2 + 2x_2z_1 + y_1z_1 + 6y_2z_2 + 2y_1z_2 + 2y\\
&\qquad\qquad = (x_1, x_2)\cdot(z_1, z_2) + (y_1, y_2)\cdot(z_1, z_2),\\
&(3)\quad \big(\alpha\,(x_1, x_2)\big)\cdot(y_1, y_2) = (\alpha\,x_1, \alpha\,x_2)\cdot(y_1, y_2) = \alpha x_1y_1 + 6\alpha x_2y_2 + 2\alpha x
\end{aligned}
$$

aby $6a^2+4a+1>0$, $\forall a \in \mathbf{R}$. Protože diskriminant této kvadratické nerov
je roven $D = 16-24 = -8 < 0$, je nerovnost $6a^2+4a+1>0$ splněna
všechna $a \in \mathbf{R}$.

Ukážeme, že předpis $(x_1,x_2)\circ(y_1,y_2) = x_1y_1+2x_2y_2+2x_1y_2+2x_2y_1$
skalárním součinem. Vlastnosti (1) až (3) jsou zřejmě splněny. Není spl
vlastnost (4), protože například

$$(-1,1)\circ(-1,1) = 1+2-2-2 = -1 \not> 0.$$

Výše uvedené příklady nás vedou k otázce, jak charakterizovat všec
skalární součiny na $\mathbf{R}^n$ a jak je rychle poznat. Souvisí to s tzv. pozitivně
finitními a symetrickými maticemi. Níže uvádím nejdůležitější výsledky z
oblasti jen pro čtenáře, který chce být lépe informován. Nám ostatním b
v dalším textu stačit existence standardního skalárního součinu na $\mathbf{R}^n$ a p
domí, že existují i jiné skalární součiny. Téma symetrických a pozitivně def
ních matic je možno přeskočit a věnovat se rovnou definici velikosti vektoru

[symmat] Čtvercová matice $\mathbf{A} \in \mathbf{R}^{n,n}$ je *symetrická*, pokud platí $\mathbf{A}^T$ =

[posdefmat] Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$ je čtvercová matice. Označme $\mathbf{A}_i \in \mathbf{R}^{n-}$
čtvercovou matici, která vzniká z matice $\mathbf{A}$ vynecháním posledních i řádk
posledních i sloupců. Matice $\mathbf{A}$ se nazývá *pozitivně definitní*, pokud všec
determinanty $\det \mathbf{A}_i$, $i \in \{0,1,2,\dots,n-1\}$ jsou kladné.

Pozitivně definitní matice je vždy regulární, protože $\det \mathbf{A} = \det \mathbf{A}_0$ >

[maticesoucinuRn] Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$ je čtvercová matice. Definujme so
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 $\boldsymbol{x}$, k
obsahuje složky vektoru $\boldsymbol{x}$, s maticí $\mathbf{A}$ a s maticí $\boldsymbol{y}^T$, což je sloupec sl

je pozitivně definitní. Na oprávněnou otázku „proč“ zde máme malý pro
pro odpověď. Odkazujeme například na učebnici [5].

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 ma
Spočteme dále jednotlivé determinanty: $\det \mathbf{A}_0 = \det \mathbf{A} = 2$, $\det \mathbf{A}_1 = \det($
1. Protože oba determinanty jsou kladná čísla, jedná se o pozitivně defin
matici. Podle věty ?? je definovaný součin skalárním součinem.

Budeme definovat velikost vektoru a úhel mezi dvěma nenulovými
tory na obecných lineárních prostorech se skalárním součinem. Tyto po
definujeme jen pomocí skalárního součinu pro zcela libovolné vektory. V na
dující kapitole ukážeme, že pokud budeme pracovat s vektory s geometrick
významem (např. s orientovanými úsečkami), pak pojmy velikost a úhel
zavedené abstraktně budou znamenat přesně to, co od nich z geometrick
hlediska očekáváme.

* [velikost] Nechť L je lineární prostor se skalárním součinem. Pro $\boldsymbol{x}$
definujeme *velikost vektoru $\boldsymbol{x}$* hodnotou $\sqrt{\boldsymbol{x} \cdot \boldsymbol{x}}$. Velikost vektoru $\boldsymbol{x}$ znač
$\|\boldsymbol{x}\|$, 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*.

[poznvelikost] Vidíme, že velikost je nezáporné číslo a že každý vektor
svou velikost. To nám zaručuje vlastnost (4) definice ??. Je $\boldsymbol{x} \cdot \boldsymbol{x} \geq 0$, ta
odmocnina z tohoto čísla je definována.

Dále vidíme, že jedině nulový vektor má velikost rovnu nule a žádný
To nám zaručuje druhá část vlastnosti (4).

[absvelikost] Nechť $\boldsymbol{x}$ je prvkem lineárního prostoru se skalárním součin

platí
$$\cos\varphi = \frac{\boldsymbol{x}\cdot\boldsymbol{y}}{\|\boldsymbol{x}\|\cdot\|\boldsymbol{y}\|}.(uhel)$$

Zabývejme se otázkou, zda každé dva nenulové vektory mají definován mezi sebou. Především podle poznámky ?? platí, že $\|\boldsymbol{x}\| \neq 0$, $\|\boldsymbol{y}\| \neq 0$, pro $\boldsymbol{x} \neq \boldsymbol{o}$, $\boldsymbol{y} \neq \boldsymbol{o}$. Takže se ve zlomku z rovnosti (??) nedělí nulou.

Aby existovalo φ takové, že platí (??), musí platit

$$-1 \leq \frac{\boldsymbol{x}\cdot\boldsymbol{y}}{\|\boldsymbol{x}\|\cdot\|\boldsymbol{y}\|} \leq 1.$$

Tento požadavek zaručuje následující věta.

* [schwartz] Nechť L je lineární prostor se skalárním součinem a $\boldsymbol{x}$ $\boldsymbol{y} \in L$. Pak platí:
$$|\boldsymbol{x}\cdot\boldsymbol{y}| \leq \|\boldsymbol{x}\|\cdot\|\boldsymbol{y}\|.(schwartz)$$

Důkaz. Nechť $\alpha \in \mathbf{R}$. Násobme sám se sebou vektor $\boldsymbol{x} - \alpha\,\boldsymbol{y}$. Podle vl nosti (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 $A = \boldsymbol{y}\cdot$ $\|\boldsymbol{y}\|^2$, $B = -2(\boldsymbol{x}\cdot\boldsymbol{y})$, $C = \boldsymbol{x}\cdot\boldsymbol{x} = \|\boldsymbol{x}\|^2$. Dostáváme

$$0 \leq A\,\alpha^2 + B\,\alpha + C.$$

Tato nerovnost musí platit pro všechna $\alpha \in \mathbf{R}$. Diskriminant této kva tické nerovnice tedy nesmí být kladný. Z toho nám vyplývá podmínka pro A, B, C:

$\|\boldsymbol{x}-\boldsymbol{y}\|$, takže často mluvíme o *vzdálenosti dvou vektorů $\boldsymbol{x}$ a $\boldsymbol{y}$* (bez závis
na jejich pořadí).

* [trojnerovnost] Pro velikosti vektorů platí

$$\|\boldsymbol{x}+\boldsymbol{y}\| \le \|\boldsymbol{x}\| + \|\boldsymbol{y}\|.(trojnerovnost)$$

Důkaz. $\|\boldsymbol{x}+\boldsymbol{y}\|^2 = (\boldsymbol{x}+\boldsymbol{y})\cdot(\boldsymbol{x}+\boldsymbol{y}) = \boldsymbol{x}\,\boldsymbol{x}+2\,\boldsymbol{x}\,\boldsymbol{y}+\boldsymbol{y}\,\boldsymbol{y} \le \|\boldsymbol{x}\|^2+2\,\|\boldsymbol{x}\|\cdot\|\boldsymbol{y}$ $\|\boldsymbol{y}\|^2 = \big(\|\boldsymbol{x}\|+\|\boldsymbol{y}\|\big)^2$. Ve výpočtu jsme použili Schwartzovu nerovnost ?? odmocnění dostáváme dokazovanou nerovnost.

Vysvětlíme si, proč se dokázaná nerovnost nazývá trojúhelníková. Tu kteří čtenáři znají geometricky formulovanou třeba takto: součet délek d stran v trojúhelníku je vždy větší než délka strany třetí. Nechť vektory a $\boldsymbol{c}$ jsou prvky lineárního prostoru se skalárním součinem a představme jako vrcholy pomyslného trojúhelníka. Velikost stran je totéž jako vzdále odpovídajících vektorů. Geometrické tvrzení o velikostech stran trojúhel tedy můžeme pomocí definice ?? přepsat takto:

$$\|\boldsymbol{a}-\boldsymbol{b}\| \le \|\boldsymbol{a}-\boldsymbol{c}\| + \|\boldsymbol{c}-\boldsymbol{b}\|.$$

Při volbě $\boldsymbol{x}=\boldsymbol{a}-\boldsymbol{c}$, $\boldsymbol{y}=\boldsymbol{c}-\boldsymbol{b}$ přechází uvedená nerovnost na tvar (??).

Uvažujme lineární prostor $\mathbf{R}^4$ se standardním skalárním součinem (Ukážeme, jak vypadá velikost vektoru $(1,2,3,4)$ a jaký je úhel mezi vek $(1,2,3,4)$ a $(1,0,0,2)$.

Podle definice ?? a podle (??) 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:

Je-li $\operatorname{hod} \mathcal{A} = 0$, pak transformace vše zobrazí do nulového vektoru. T
vou transformaci zapíšeme jako změnu měřítka s koeficienty $0, 0$.

Je-li $\operatorname{hod} \mathcal{A} = 1$, pak transformace $\mathcal{A}$ je projekce. Jádrem zobrazení
vektory v jedné přímce. Aplikujme otočení, které zajistí, že tato přímka se k
s první souřadnicovou osou. Pak aplikujeme změnu měřítka s koeficientem
(jak zvolit parametr r je popsáno níže). Nakonec druhou souřadnicovou
otočíme tak, aby se kryla s $\mathcal{A}(U_O)$.

Je-li $\operatorname{hod} \mathcal{A} = 2$, pak dva na sebe kolmé bázové vektory s jednotko
velikostí se zobrazí na dva lineárně nezávislé vektory $\boldsymbol{b}_1', \boldsymbol{b}_2'$. Pokusíme se
vektory transformovat zpět pomocí otočení a změny měřítka na původní bá
vektory. Tím popíšeme $\mathcal{A}^{-1}$. Protože inverze k otočení je otočení a inverz
změně měřítka s nenulovými koeficienty je změna měřítka, je možné zapsat
složení těchto transformací i původní transformaci $\mathcal{A}$.

Nejprve aplikujeme otočení, které způsobí, že delší z vektorů $\boldsymbol{b}_1', \boldsymbol{b}_2'$ se k
s první souřadicovou osou. Pak aplikujeme změnu měřítka s koeficienty
která nemění delší z vektorů. Parametr t volíme tak, aby po změně měřítka
(původně) kratší vektor stejnou velikost, jako jeho delší bráška. Dále proved
otočení tak, aby osa úhlu těchto vektorů se kryla s první osou. Poté proved
změnu měřítka s parametry $u, 1$, aby sledované vektory byly na sebe ko
Dále otočíme tyto vektory tak, aby se kryly s osami a nakonec proved
změnu měřítka tak, aby měly jednotkovou velikost.

Jak zvolíme parametr r? Zvolme vektor $\boldsymbol{w}$, který leží v $\mathcal{A}(U_O)$ a má
notkovou velikost. Jeho obraz $\mathcal{A}(\boldsymbol{w})$ také leží na přímce $\mathcal{A}(U_O)$, takže
$\mathcal{A}(\boldsymbol{w}) = r\,\boldsymbol{w}$. Parametr r je tedy velikost obrazu $\mathcal{A}(\boldsymbol{w})$.

Jak zvolíme paramter t? Nechť delší vektor má velikost v a kratší ve
má souřadnice (a, b) vzhledem k bázi (B). Po změně měřítka má tento ve
souřadnice (a, tb) a má tedy velikost $\sqrt{a^2 + t^2 b^2}$, což se musí rovnat v. Ta

měřítka s parametry $u, 1$ budou mít tyto vektory souřadnice (ua, b), $(ua,$
Mají být na sebe kolmé, tedy skalární součin těchto vektorů má být nulov

$$(ua, b) \cdot (ua, -b) = u^2a^2 - b^2 = 0, \quad \text{takže} \quad u^2a^2 = b^2, \quad u = \frac{b}{a}.$$

[sskonv] Nechť L je lineární prostor spojitých funkcí definovaných na
nečném 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
Nechť $f \in L$, $g \in L$, $h \in L$ a $\alpha \in \mathbf{R}$. Pak platí

$$(1) \quad f \cdot g = \int_D f(x)\, g(x)\, \mathrm{d}x = \int_D g(x)\, f(x)\, \mathrm{d}x = g \cdot f,$$

$$(2) \quad (f+g) \cdot h = \int_D \big(f(x) + g(x)\big)\, h(x)\, \mathrm{d}x = \int_D \big(f(x)\, h(x) + g(x)\, h(x)\big)\, \mathrm{d}$$

$$= \int_D f(x)\, h(x)\, \mathrm{d}x + \int_D g(x)\, h(x)\, \mathrm{d}x = f \cdot h + g \cdot h,$$

$$(3) \quad (\alpha f) \cdot g = \int_D \alpha f(x)\, g(x)\, \mathrm{d}x = \alpha \cdot \int_D f(x)\, g(x)\, \mathrm{d}x = \alpha\, (f \cdot g),$$

$$(4) \quad f \cdot f = \int_D f^2(x)\, \mathrm{d}x \ge 0,$$

$$\int_D f^2(x)\, \mathrm{d}x = 0 \quad \text{jen tehdy, když } f(x) = 0\ \forall x \in D, \text{prot}$$

Příklad ilustruje, že i na lineárních prostorech nekonečné dimenze jsme sch

Protože máme na lineárních prostorech se skalárním součinem defino úhel mezi nenulovými vektory, můžeme pro každé dva nenulové vektory rozh nout, kdy jsou na sebe kolmé. Je to tehdy, když je $\cos\varphi = 0$, neboli $\boldsymbol{x} \cdot \boldsymbol{y}$ Z toho vyplývá následující definice.

[kolmost] Nechť L je lineární prostor se skalárním součinem. Dva nenu vektory $\boldsymbol{x} \in L$ a $\boldsymbol{y} \in L$ *jsou na sebe kolmé* (značíme $\boldsymbol{x} \perp \boldsymbol{y}$), pokud je $\boldsymbol{x} \cdot \boldsymbol{y}$

(Pythagorova věta.) Nechť $\boldsymbol{x} \in L$, $\boldsymbol{y} \in L$ jsou nenulové vektory, které na sebe kolmé. Pak platí

$$\|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2 = \|\boldsymbol{x} - \boldsymbol{y}\|^2.$$

Zdůvodnění je jednoduché: $\|\boldsymbol{x}-\boldsymbol{y}\|^2 = (\boldsymbol{x}-\boldsymbol{y})\cdot(\boldsymbol{x}-\boldsymbol{y}) = \boldsymbol{x}\cdot\boldsymbol{x} - 2\boldsymbol{x}\cdot\boldsymbol{y} + \boldsymbol{y}\cdot$ $\|\boldsymbol{x}\|^2 - 2\cdot 0 + \|\boldsymbol{y}\|^2$. Geometrická interpretace tohoto příkladu je následu Trojúhleník s vrcholy $\boldsymbol{o}$, $\boldsymbol{x}$ a $\boldsymbol{y}$ je pravoúhlý s pravým úhlem při vrchol Čísla $\|\boldsymbol{x}\|$, $\|\boldsymbol{y}\|$ jsou velikosti odvěsen a $\|\boldsymbol{x}-\boldsymbol{y}\|$ je velikost přepony.

* [ortonormalni] Nechť $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n\}$ je báze lineárního pros se skalárním součinem. Bázi B nazýváme *ortogonální*, pokud $\boldsymbol{b}_i \perp \boldsymbol{b}_j$ $\forall$ $\{1, 2, \dots, n\}$, $\forall j \in \{1, 2, \dots, n\}$, $i \neq j$.

Bázi B nazýváme *ortonormální*, pokud je ortogonální, a navíc $\|\boldsymbol{b}_i\|$ = $\forall i \in \{1, 2, \dots, n\}$.

[ortobase] Báze $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n\}$ je ortonormální právě tehdy, kdy

$$\boldsymbol{b}_i \cdot \boldsymbol{b}_j = \begin{cases} 0 \text{ pro } i \neq j, \\ 1 \text{ pro } i = j. \end{cases}$$

Důkaz. Báze B je ortonormální právě tehdy, když (podle definice ??) p $\boldsymbol{b}_i \cdot \boldsymbol{b}_j = 1$ pro $i = j$ a navíc je ortogonální, tj. $\boldsymbol{b}_i \perp \boldsymbol{b}_j$ pro $i \neq j$. To p definice ?? znamená, že $\boldsymbol{b}_i \cdot \boldsymbol{b}_j = 0$ pro $i \neq j$.

Důkaz. Podle předpokladu je $\boldsymbol{x} = x_1\,\boldsymbol{b}_1 + x_2\,\boldsymbol{b}_2 + \cdots + x_n\,\boldsymbol{b}_n$, $\boldsymbol{y} = y_1\,$ $y_2\,\boldsymbol{b}_2 + \cdots + y_n\,\boldsymbol{b}_n$. Počítejme $\boldsymbol{x}\cdot\boldsymbol{y}$:

$$\boldsymbol{x}\cdot\boldsymbol{y} = (x_1\,\boldsymbol{b}_1 + x_2\,\boldsymbol{b}_2 + \cdots + x_n\,\boldsymbol{b}_n)\cdot(y_1\,\boldsymbol{b}_1 + y_2\,\boldsymbol{b}_2 + \cdots + y_n\,\boldsymbol{b}_n) =$$
$$= x_1y_1\,\boldsymbol{b}_1\cdot\boldsymbol{b}_1 + x_1y_2\,\boldsymbol{b}_1\cdot\boldsymbol{b}_2 + \cdots + x_1y_n\,\boldsymbol{b}_1\cdot\boldsymbol{b}_n + x_2y_1\,\boldsymbol{b}_2\cdot\boldsymbol{b}_1 + x_2y_2\,\boldsymbol{b}_2\cdot\boldsymbol{b}_2 + \cdots + x_2y$$
$$= x_1y_1\cdot 1 + x_1y_2\cdot 0 + \cdots + x_1y_n\cdot 0 + x_2y_1\cdot 0 + x_2y_2\cdot 1 + \cdots + x_2y_n\cdot 0 + \cdots + x_ny_n\cdot 1 =$$

V úpravách jsme využili větu ?? a toho, že báze B je ortonormální.

Nechť $\mathbf{R}^n$ je lineární prostor se standardním skalárním součinem zav ným 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.

* [kolmeLN] Nechť $\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_n$ jsou nenulové vektory lineárního storu se skalárním součinem, které jsou na sebe navzájem kolmé, tj. $\boldsymbol{x}_i\cdot\boldsymbol{x}_j$ 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 str uvedené rovnosti skalárně vektorem $\boldsymbol{x}_i$, dostáváme na levé straně součet s výjimkou jediného sčítance, protože vektor $\boldsymbol{x}_i$ je kolmý na všechny všec ostatní vektory $\boldsymbol{x}_j$. Máme tedy

$$\alpha_i\,\boldsymbol{x}_i\cdot\boldsymbol{x}_i = \boldsymbol{o}\cdot\boldsymbol{x}_i = 0.$$

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
nice souřadnic vzhledem k bázi máme dokázat, že $\boldsymbol{x} = \boldsymbol{y}$. Násobme vekt
vektorem $\boldsymbol{b}_i$:

$$\boldsymbol{y} \cdot \boldsymbol{b}_i = \big((\boldsymbol{x} \cdot \boldsymbol{b}_1)\, \boldsymbol{b}_1 + (\boldsymbol{x} \cdot \boldsymbol{b}_2)\, \boldsymbol{b}_2 + \cdots + (\boldsymbol{x} \cdot \boldsymbol{b}_n)\, \boldsymbol{b}_n\big) \cdot \boldsymbol{b}_i = (\boldsymbol{x} \cdot \boldsymbol{b}_i)\, \boldsymbol{b}_i \cdot \boldsymbol{b}_i = \boldsymbol{x}$$

protože báze (B) je ortonormální. Máme tedy výsledek $\boldsymbol{x} \cdot \boldsymbol{b}_i = \boldsymbol{y} \cdot \boldsymbol{b}_i$
$\{1, 2, \ldots, n\}$.

Vektor $\boldsymbol{x} - \boldsymbol{y}$ je kolmý na všechny prvky $\boldsymbol{b}_i$, protože z předchozího výp
plyne $(\boldsymbol{x} - \boldsymbol{y}) \cdot \boldsymbol{b}_i = 0$. Pokud by $\boldsymbol{x} \neq \boldsymbol{y}$, pak podle věty ?? jsou vek
$\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n, \boldsymbol{x} - \boldsymbol{y}$ lineárně nezávislé, ale to je ve sporu s tím, že (B) je b
Musí tedy být $\boldsymbol{x} = \boldsymbol{y}$.

Předchozí věta má názornou geometrickou interpretaci. Souřadnice $\boldsymbol{x}$
jsou vlastně kolmé průměty vektoru $\boldsymbol{x}$ na vektory báze $\boldsymbol{b}_i$. O těchto pojm
pohovoříme podrobněji v následující kapitole.

[uhly-k-osam] Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je ortonormální báze lineár
prostoru se skalárním součinem a $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)_{(B)}$ je jeho libov
vektor. Pak úhel φ_i mezi vektorem $\boldsymbol{x}$ a vektorem $\boldsymbol{b}_i$ lze počítat podle vzo

$$\cos \varphi_i = \frac{x_i}{\|\boldsymbol{x}\|}\,.$$

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 $x_i = \boldsymbol{x} \cdot \boldsymbol{b}_i$.

Protože je $\|\boldsymbol{x}\|^2 / \|\boldsymbol{x}\|^2 = 1$ a dále je $\|\boldsymbol{x}\|^2 = x_1^2 + x_2^2 + \cdots + x_n^2$, ply

Následující věta ukazuje, že každá konečná báze se dá v jistém smyslu pozm
tak, aby se z ní stala ortonormální báze.

* [ortogonalizace] Nechť $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ je báze lineárního prostoru
skalárním součinem. Pak existuje ortonormální báze $\{\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n\}$ takova

$$\langle \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k \rangle = \langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k \rangle, \qquad \forall k \in \{1, 2, \ldots, n\}.$$

Důkaz. Nejprve vysvětlíme ideu důkazu, která je v tomto případě asi důleži
než podrobné počítání. Vektor $\boldsymbol{c}_1$ volíme stejný jako $\boldsymbol{b}_1$ jen s tím rozdílem
jej „normalizujeme“. To znamená, že jej násobíme vhodnou konstantou,
$\|\boldsymbol{c}_1\| = 1$.

Představme si dále, že už jsme našli $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$ takové, že $\langle \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots,$
$\langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k \rangle$, a přitom vektory $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$ jsou na sebe vzájemně kolm
mají jednotkovou velikost. Vektor $\boldsymbol{b}_{k+1}$ nyní „ortogonalizujeme“, tj. uprav
tak, aby byl kolmý na všechny vektory z $\langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k \rangle$. Ukážeme později
k tomu účelu stačí od vektoru $\boldsymbol{b}_{k+1}$ odečíst určitou lineární kombinaci
torů $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$. Takto upravený vektor dále „normalizujeme“, tj. vyn
bíme vhodnou konstantou, aby $\|\boldsymbol{c}_{k+1}\| = 1$. Tím se jeho kolmost vůči ostat
vektorům z $\langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k \rangle$ nepokazí. Protože vektor $\boldsymbol{c}_{k+1}$ vznikl jako line
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
vektor. Opakovaným použitím tohoto postupu dostáváme hledanou orto
mální bázi $\{\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n\}$.

Nyní stačí jen podrobněji ukázat, jak se vektor „normalizuje“ a „o
gonalizuje“. Normalizaci libovolného vektoru $\boldsymbol{x}$ provedeme tak, že polož
$\boldsymbol{x}' = (1/\|\boldsymbol{x}\|) \cdot \boldsymbol{x}$. Skutečně je:

$$\|\boldsymbol{x}'\|^2 = \boldsymbol{x}' \cdot \boldsymbol{x}' = \frac{1}{\|\boldsymbol{x}\|}\,\boldsymbol{x} \cdot \frac{1}{\|\boldsymbol{x}\|}\,\boldsymbol{x} = \frac{1}{\|\boldsymbol{x}\|^2}\,\boldsymbol{x}\,\boldsymbol{x} = \frac{1}{\|\boldsymbol{x}\|^2}\,\|\boldsymbol{x}\|^2 = 1.$$

Nově vytvořený vektor $\boldsymbol{b}'_{k+1}$ je kolmý na všechny vektory $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$, prot

$$\boldsymbol{b}'_{k+1} \cdot \boldsymbol{c}_j = \left(\boldsymbol{b}_{k+1} - \sum_{i=1}^{k} (\boldsymbol{b}_{k+1} \cdot \boldsymbol{c}_i)\, \boldsymbol{c}_i \right) \cdot \boldsymbol{c}_j = \boldsymbol{b}_{k+1} \cdot \boldsymbol{c}_j - \sum_{i=1}^{k} (\boldsymbol{b}_{k+1} \cdot \boldsymbol{c}_i)\, (\boldsymbol{c}_i \cdot \boldsymbol{c}_j) =$$

V uvedeném součtu jsou ostatní sčítanci nuloví, protože vektory $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots$ jsou podle předpokladu na sebe navzájem kolmé.

[dortomat] Matice $\mathbf{A} \in \mathbf{R}^{n,n}$, pro kterou platí $\mathbf{A}^T \cdot \mathbf{A} = \mathbf{E}$, se na *ortogonální*.

[ortomat-zaklad] Nechť $\mathbf{A} \in \mathbf{R}^{n,n}$. V $\mathbf{R}^n$ předpokládejme standardní lární 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 orto málni bázi.

Důkaz. (1)⇒(2): Protože $\mathbf{A}^T \cdot \mathbf{A} = \mathbf{E}$, je $\mathbf{A}$ regulární a $\mathbf{A}^{-1} = \mathbf{A}^T$. Inve 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 $\mathbf{A} = (\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots$ 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 stand skalární součin v $\mathbf{R}^n$.

(4)⇔(5): protože (1)⇔(3).

(6)$\Leftrightarrow$(7): Viz definici matice přechodu ??.

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:

$$\begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Tyto matice jsou maticemi transformací, které zobrazují ortonormální báz ortonormální bázi (transformace zachovává velikosti a úhly).

[ortomat] (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 ste 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): $\|\mathbf{A}\mathbf{x}\|^2 = (\mathbf{A}\mathbf{x})^T \cdot (\mathbf{A}\mathbf{x}) = \mathbf{x}^T \cdot \mathbf{A}^T \cdot \mathbf{A} \cdot \mathbf{x} = \mathbf{x}^T \cdot \mathbf{x} = \|\mathbf{x}\|^2$.

[QR] Je-li $\mathbf{A}$ regulární matice, pak existuje ortogonální matice $\mathbf{Q}$ a h 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 Sch dtovým ortogonalizačním procesem ?? na ortonormální bázi (C). Bázi $(C$ píšeme do sloupců matice $\mathbf{Q}$. Matice $\mathbf{R}$ je maticí přechodu od ortonorm

Ortogonální matice jsou hojně používány v numerických metodách, ne
jsou numericky stabilní. Díky (3) věty ?? se totiž násobením ortogonální ma
chyba nezvětšuje.

Věta o QR rozkladu je jen jiný pohled na Schmidtův ortogonalizační
ces. Říká, že máme-li ve sloupcích matice $\mathbf{A}$ nějakou bázi, pak ji můžeme
rovnat", aby byla ortonormální a takto opravenou bázi zapsat do matice
Přitom matice $\mathbf{R}$ je maticí koeficientů tohoto „narovnání".

Dá se ukázat, že ortonogonální matice je vždy maticí nějakého oto
(při větší dimenzi je možné otáčet v různých směrech). Toto otočení je přípa
složeno s osovou souměrností (ve více dimenzích překlopením jednoho bázov
vektoru do „protisměru").

V případě matic $\mathbf{A} \in \mathbf{C}^{n,n}$ je analogií ortogonální matice tzv. *unit*
matice definovaná v ??. Důvod použití komplexně sdružených čísel v def
unitární matice souvisí s axiomem (1) skalárního součinu ??, který je pro k
plexní čísla modifikován v souladu s poznámkou ??.

[unitarmat] Matice $\mathbf{A}^H \in \mathbf{C}^{n,m}$ se nazývá *Hermitovsky sdružená* k ma
$\mathbf{A} \in \mathbf{C}^{m,n}$ pokud je transponovaná a místo každého prvku je v matici zap
prvek komplexně sdružený.

Matice $\mathbf{A} \in \mathbf{C}^{n,n}$ se nazývá *unitární*, pokud $\mathbf{A}^H \cdot \mathbf{A} = \mathbf{E}$.

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 m
velikosti vektorů /??/ a úhly mezi nenulovými vektory /??/. Abychom
jistotu, že vzorec pro úhel dává výsledek pro libovolné nenulové vektory, mu
jsme dokázat Schwartzovu nerovnost /??/.

Dva nenulové vektory jsou na sebe kolmé, právě když jejich skalární so
je roven nule. Zavedli jsme ortonormální bázi /??/ a ukázali důležité vlastn
této báze /??, ??, ??/.

14. Polynomy

S polynomy jsme se v tomto textu už na mnoha místech setkali. Praco
jsme s nimi jako s funkcemi danými jistým vzorcem a shledali jsme, že mno
polynomů tvoří lineární prostor. V této kapitole se na polynomy podív
poněkud důkladněji a budeme vyšetřovat zejména vlastnosti jejich kořenů

Na polynom se můžeme dívat dvěma pohledy. Buď jako na funkci da
jistým vzorcem (definice ??) nebo polynom ztotožníme s tím vzorečkem
motným (definice ??). Každý přístup vede k jinému způsobu porovnávání d
polynomů, sčítání polynomů a násobení polynomu konstantou nebo poly
mem.

Zavedeme tedy lineární prostor polynomů jednak jako podprostor fu
se sčítáním a násobením obvyklým pro funkce. Dále zavedeme jiný lineární
stor polynomů jako vzorečků se sčítáním a násobením těch vzorečků. Nak
ukážeme, že tyto dva lineární prostory jsou izomorfní, tedy, že mezi polyn
jako funkcemi a polynomy jako vzorečky existuje vzájemně jednoznačný vz

Pokud se čtenář nechce zatěžovat intuitivně samozřejmými úvahami o t
že polymom vnímaný jako vzoreček podle definice ?? je víceméně totéž
polynom vnímaný jako funkce podle definice ??, může následující text přesk
a pokračovat až definicí ??.

[dpolf] *Polynom* je reálná funkce reálné proměnné, tedy $p\colon \mathbf{R} \to \mathbf{R}$, k
má pro všechna $x \in \mathbf{R}$ funkční hodnotu $p(x)$ danou vzorcem

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, (defpol)$$

kde $a_0, \ldots, a_n$ jsou nějaká reálná čísla, která nazýváme *koeficienty* polyno
Jinými slovy: je-li funkce p polynomem, existuje přirozené číslo n a konsta
$a_0, \ldots, a_n$ tak, že pro funkční hodnoty $p(x)$ platí uvedený vzorec pro všec
$x \in \mathbf{R}$.

[polfukc] Dva polynomy p a q podle této definice se rovnají, pokud

že je zde použit vzorec (??) v opačném pořadí „od nejvyšší mocniny promě
k mocninám nižším". Toto je dost častý zápis vzorců pro polynomy. Vzhle
k tomu, že sčítání reálných čísel je komutativní, na pořadí sčítanců nezále

Funkce exp, jejíž hodnota v bodě $x \in \mathbf{R}$ je daná vzorcem $\exp(x) = e^x$,
polynom. To znamená, že neexistuje konečné množství konstant $a_0, a_1, \ldots$
takové, že e^x lze vypočítat podle vzorce (??) pro všechny $x \in \mathbf{R}$. Abych
to dokázali, vypůjčíme si znalosti z analýzy. Je zřejmé, že pokud opako
derivujeme vzorec (??) podle proměnné x více než n krát, dostáváme nul
funkci. Takže každý polynom p má tu vlastnost, že pro něj existuje přiro
číslo k takové, že k-tá derivace polynomu p je nulová funkce. Je známo, že fu
exp je odolná vůči libovolnému množství derivování: dostáváme zase fu
exp, která je nenulová. Takže tato funkce nemůže být polynom. Z analogick
důvodů například funkce sinus a kosinus nejsou polynomy. Poznamenejme je
že hodnoty uvedených funkcí se dají přibližně počítat pomocí polynomů (
Taylorovy polynomy). Toto téma ovšem překračuje rámec tohoto textu.

Následuje alternativní definice polynomu, v algebře možná obvyklejší

[dpolv] *Polynom* je vzoreček

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, (defpolv)$$

kde $a_0, \ldots, a_n$ jsou nějaká reálná čísla, která nazýváme *koeficienty* polyn
a x je formální proměnná (která samozřejmě může být označena jiným pís
nem).

Polynom v tomto pojetí je určen jednoznačně konečně mnoha koefici
$a_0, \ldots, a_n$, pomocí kterých lze uvedený vzoreček sestavit.

Hodnota polynomu s koeficienty $a_0, \ldots, a_n$ v bodě α je číslo $a_0 + a_1$
$a_2\alpha^2 + \cdots + a_n\alpha^n$.

[polvplus] Předpokládejme definici polynomů ??. Nechť polynom p má
ficienty $a_0, \ldots, a_m$ a polynom q má koeficienty $b_0, \ldots, b_n$. Bez újmy na obecn

pracovat s polynomy jen pomocí jejich koeficientů. Nemusejí implement
kompletně celý vzoreček (??).

Dva polynomy $0x^3 + 0x^2 - 2x + 3$ a $-2x + 3$ se rovnají, ačkoli ten prvn
čtyři koeficienty a ten druhý jen dva. Koeficienty a_0 a a_1 mají ale oba polyn
stejné.

Součtem polynomů $x^3 + 3x^2 - 2x$ a $5x + 7$ je polynom $x^3 + 3x^2 + 3x$
protože má následující koeficienty (po řadě od koeficientu s indexem nu
$0 + 7$, $-2 + 5$, 3, 1.

[PX] Množina vzorečků tvaru (??), ve které dva vzorečky považujem
totožné podle pravidla v definici ?? a na které je definováno sčítání a n
bení konstantou podle stejné definice ??, tvoří lineární prostor. Tuto mno
označíme symbolem $\mathcal{P}_X$.

Důkaz. Součet dvou prvků z $\mathcal{P}_X$ je prvek v $\mathcal{P}_X$, α-násobek prvku z $\mathcal{P}$
prvek v $\mathcal{P}_X$. Dále je třeba ověřit platnost axiomů (1) až (7) z definice ??
přenecháme pečlivému čtenáři.

Definice ?? rovnosti, součtu a násobku vychází přirozeně z toho, jak byc
porovnávali, sčítali a násobili vzorečky tvaru (??). Je to ovšem jiná defi
než vyplývá z poznámky ??. Určitou práci nám dá uvést oba tyto svět
souvislosti.

V definici ?? mluvíme o *hodnotě polynomu*. Tím je každému reáln
číslu α přiřazena funkční hodnota polynomu, tedy polynom daný vzorečke
stává funkcí. To popisuje jednoznačný přechod od polynomu v podobě vzor
k polynomu jako funkci. Ukazuje se, že obráceně (od funkce ke vzorečku)
malinko složitější:

[poljeden] Každá funkce $p\colon \mathbf{R} \to \mathbf{R}$, která je polynomem podle definice
má své koeficienty určeny jednoznačně. Přesněji: pokud funkce p je polyno
jednak s koeficienty $a_0, \ldots, a_m$ a také s koeficienty $b_0, \ldots, b_n$, pak pro
koeficienty platí rovnost podle definice ??.

do vzorce dosadit $x = 0$). Protože $p(0) = 0$, je nutně $a_0 = 0$. Hodnotu fu
p v bodě x můžeme tedy zapsat ve tvaru:

$$0 = p(x) = x\,(a_1 + a_2x + \ldots + a_nx^{n-1}) = x \cdot q(x).$$

Polynom q musí mít nulové hodnoty pro všechna $x \neq 0$. Protože q je spo
funkce, je také $q(0) = 0$. Po dosazení $x = 0$ do vzorce pro $q(x)$ dostáv
$a_1 = 0$. Nyní můžeme psát

$$0 = p(x) = x^2(a_2 + a_3x + \ldots + a_nx^{n-1}) = x^2 \cdot q_2(x)$$

a úvahu můžeme zopakovat. Dostáváme $a_2 = 0$. Matematickou indukc
ukázat, že $a_k = 0$ pro všechna $k \in \{0, 1, \ldots, n\}$.

Pokračování důkazu věty ??. Nechť $p(x) = a_0 + a_1x + \cdots + a_mx^{r}$
$b_0+b_1x+\cdots+b_nx^n$ pro všechna $x \in \mathbf{R}$. Bez újmy na obecnosti lze předpokla
$m \leq n$. Odečtením dostaneme

$$p(x){-}p(x) = (b_0{-}a_0){+}(b_1{-}a_1)\,x{+}\ldots{+}(b_m{-}a_m)\,x^m{+}b_{m+1}x^{m+1}{+}\ldots{+}b_nx^{n}$$

což je nulová funkce. Podle věty ?? má tento nulový polynom všechny koe
enty nulové, tedy musí $a_k = b_k$ pro všechna $k \in \{0, 1, \ldots, m\}$ a musí b_k
pro všechna $k \in \{m+1, \ldots, n\}$.

[pollin] Zobrazení z lineárního prostoru $\mathcal{P}_X$ (viz větu ??) do lineár
prostoru funkcí, které vzorečku (??) přiřadí funkci $p\colon \mathbf{R} \to \mathbf{R}$ předpisem (
je lineární.

Důkaz. Je třeba dokázat, že součtem polynomů p a q podle definice ??
stáváme polynom $p + q$, pro který platí $(p + q)(x) = p(x) + q(x)$ pro vše
$x \in \mathbf{R}$. Nechť polynom p má koeficienty $a_0, \ldots, a_m$ a polynom q má koefic
$b_0, \ldots, b_n$. Bez újmy na obecnosti lze předpokládat $m \leq n$. Je

pro všechna $x \in \mathbf{R}$, jinými slovy $\alpha\, p(x) = (\alpha p)(x)$ pro všechna $x \in \mathbf{R}$. Zobra
je tedy lineární.

[polyniso] Zobrazení z lineárního prostoru $\mathcal{P}_X$ (viz větu ??) do lineár
prostoru polynomů jako funkcí, které vzorečku přiřadí funkci předpisem (
je izomorfismus.

Důkaz. Zmíněné zobrazení je prosté (věta ??), je na (protože každý poly
jako funkce má svůj vzoreček) a je lineární (věta ??).

Důsledkem této věty je tvrzení, že součet polynomů (jako funkce) je
lynom a také α-násobek polynomu je polynom. Stačí od funkcí přejít po
inverzního izomorfismu ke vzorečkům, tam provést součet (nebo α-násobe
výsledek přenést zpět do prostoru polynomů jako funkcí.

[defstup] Nechť polynom p má koeficienty $a_0, a_1, \dots, a_n$. *Stupeň polyn*
je největší index k takový, že $a_k \neq 0$. Má-li polynom všechny koeficienty nu
(tzv. *nulový polynom*), prohlásíme, že jeho stupeň je roven -1.

Polynom $0x^5 + 0x^4 + 5x^3 - 4x^2 + 2x + 7$ má koeficienty $a_0 = 7$, a_1
$a_2 = -4$, $a_3 = 5$, $a_4 = 0$, $a_5 = 0$. Takže největší index nenulového koefici
je 3. Polynom má stupeň tři.

Součin polynomů p a q je funkce u daná předpisem $u(x) = p(x)\, q(x)$
všechna $x \in \mathbf{R}$. Součin polynomů p a q značíme pq.

[psoucin] Nechť p má koeficienty $a_0, a_1, \dots, a_m$ a q má koeeficienty b_0, b_1
Pak součin polynomů pq je polynom s koeficienty c_k pro $k \in \{0, 1, \dots, m$
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 $p(x) = a_0 + a_1 x + \cdots + a_m x^m$ a $q(x) = b_0 + b_1 x + \cdots + b_n x^n$.
všechna $x \in \mathbf{R}$ spočítáme $p(x)\, q(x)$. Pro větší pohodlí přitom značíme a_i
pro $i > m$ a $b_i = 0$ pro $i > n$.

to polynom stupně -1 pro $\alpha = 0$. Konečně pro nenulové polynomy p a q j
polynom stupně $m+n$. Je-li p nebo q nulový, pak pq je polynom stupně -

Důkaz. Tvrzení plyne přímo z vět o počítání koeficientů součtu a sou
polynomů a z definice stupně polynomu.

Je potřeba si uvědomit, že stupeň součtu polynomů nemusí dosah
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
domit, že stupeň součtu určitě nabývá maxima stupňů jednotlivých polyno
které sčítáme, pokud stupně sčítaných polynomů jsou různé.

[castecnypodilp] Podíl dvou polynomů (definovaný jako podíl funkcí)
musí být polynom. Nechť jsou dány polynomy p a q, přitom q je nenulov
možné provést aspoň částečný podíl těchto polynomů se zbytkem, tedy n
takové polynomy r a z, aby polynom z měl menší stupeň než q a aby plat

$$\frac{p(x)}{q(x)} = r(x) + \frac{z(x)}{q(x)}$$

pro všechna $x \in \mathbf{R}$ taková, že $q(x) \neq 0$. V tomto kontextu říkáme polynom
částečný podíl polynomů p a q. Polynomu z říkáme *zbytek* po dělení polyn
p polynomem q. Následující věta ukazuje, že pro každé polynomy p a
nenulový) existuje jejich částečný podíl a zbytek po jejich dělení. Přitom
polynomy r a z určeny jednoznačně.

[delenip] Nechť p, q jsou polynomy, q nenulový. Pak existuje právě je
polynom r a právě jeden polynom z tak, že (i) $p = rq + z$, (ii) stupeň z je m
než stupeň 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 inde m (koeficient u nejvyšší mocniny). Platí $m \geq n$, protože není spl podmínka z kroku (2). K polynomu r přičteme polynom daný vzor $(d/c)\, x^{m-n}$ a od polynomu z odečteme polynom daný vzorcem $(d/c)\, x^{m}$ Vznikají nové polynomy r_1 a z_1, které dále označíme r a z a vracíme s kroku (2).

V kroku (3) se snižuje stupeň polynomu z, protože se od tohoto polyn odečítá sčítanec s nejvyšší mocninou. Tím je zaručeno, že stupeň polyn z postupně klesá a algoritmus určitě skončí. Krok (2) navíc zaručuje, ž splněno (ii) z tvrzení věty. Další vlastností algoritmu je skutečnost, že v kaž okamžiku platí pro polynomy r a z podmínka (i), takže tato podmínk splněna i po ukončení algoritmu. Především v kroku (1) je $r = 0$ a $z = p$, t $rq + z = 0q + p = p$ a podmínka (i) je splněna. Dále v kroku (3) máme zaruč že $p = rq + z$ a ukážeme, že platí také $p = r_1 q + z_1$. Pro všechna $x \in \mathbf{R}$ je

$$r_1(x)\, q(x) + z_1(x) = \left(r(x) + \frac{d}{c}\, x^{m-n} \right) q(x) + \left(z(x) - \frac{d}{c}\, x^{m-n}\, q(x) \right) =$$

$$= r(x)\, q(x) + \frac{d}{c}\, x^{m-n}\, q(x) + z(x) - \frac{d}{c}\, x^{m-n}\, q(x) = r(x)$$

Jednoznačnost polynomů r a z je jednoduchým důsledkem věty o st součtu a součinu polynomů. Kdyby existovaly polynomy r_2 a z_2, které ro splňují (i) a (ii), pak je $p = rq + z = r_2 q + z_2$, takže $(r - r_2)\, q = z_2$ Kdyby $r - r_2$ nebyl nulový polynom, pak stupeň polynomu $(r - r_2)q$ by větší nebo roven stupni q, zatímco polynom $z_2 - z$ má stupeň menší než q

schématu:

$$
\begin{array}{r}
(2x^5 - 3x^4 + 3x^3 - x^2 - 6x + 8) : (x^2 - 2x + 4) = 2x^3 + x^2 - 3x - 1 \\
-(2x^5 - 4x^4 + 8x^3) \phantom{- x^2 - 6x + 8) : (x^2 - 2x + 4) = 2x^3 + x^2 - 3x - 1} \\
\hline
x^4 - 5x^3 - x^2 - 6x + 8 \\
-(x^4 - 2x^3 + 4x^2) \phantom{- 6x + 8} \\
\hline
-3x^3 - 5x^2 - 6x + 8 \\
-(-3x^3 + 6x^2 - 12x) \phantom{+ 8} \\
\hline
-11x^2 + 6x + 8 \\
-(-11x^2 + 22x - 44) \\
\hline
-16x + 52
\end{array}
$$

V prvním řádku (před symbolem „:“) je výchozí hodnota polynomu z p
kroku (1). Sčítanec s nejvyšší mocninou polynomu z je $2x^5$ a ten podě
prvním sčítancem polynomu q, tj. x^2. Výsledek zapíšeme vedle rovnítka:
Tímto výsledkem násobíme celý polynom q a píšeme pod výchozí polyno
do druhého řádku. Tyto dva polynomy odčítáme a výsledek píšeme pod č
Vzniká nová hodnota polynomu z. Sčítanec s nejvyšší mocninou je nyní x^4 a
znovu dělíme x^2 a výsledek $+x^2$ připisujeme vedle rovnítka. Tímto výsled
znovu násobíme celý polynom q a píšeme do čtvrtého řádku. Pod čáru zapíš
do pátého řádku rozdíl, tedy novou hodnotu polynomu z. Postupujeme
dlouho, dokud polynom z má stupeň větší nebo roven stupni polynom
Teprve na devátém řádku jsme dosáhli skutečného zbytku, neboť nyní t
polynom má stupeň menší než stupeň polynomu q. Výsledek částečného po
můžeme zapsat takto:

$$\frac{2x^5 - 3x^4 + 3x^3 - x^2 - 6x + 8}{\cdots} = 2x^3 + x^2 - 3x - 11 + \frac{-16x + 52}{\cdots}$$

funkci f, jejíž hodnoty $f(x)$ jsou rovny podílu $p(x)/q(x)$ všude tam, kde $q($
0, pak bychom nemuseli dostat polynom, protože definiční obor takové funk
nemusí obsahovat všechna reálná čísla **R**. Pravda, pokud je polynom p dělit
polynomem q, pak funkci f lze spojitě dodefinovat v bodech x, pro kter
$q(x) = 0$. Takto rozšířená funkce f je pak totožná s podílem polynomů p
předchozí definice ??. To plyne z následující věty.

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 dokazov
tvrzení je vlastnost (i) uvedené věty.

Nechť je dán polynom p svými koeficienty $a_0, a_1, \ldots, a_n$. K nalezení h
noty $p(\alpha)$ můžeme použít jednak vzorec (??)

$$p(\alpha) = a_n \alpha^n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_2\alpha^2 + a_1\alpha + a_0 (amaterp$$

nebo můžeme tento vzorec přezávorkovat do tvaru

$$p(\alpha) = ((\cdots((a_n\alpha + a_{n-1})\,\alpha + a_{n-2})\,\alpha + \cdots + a_2)\,\alpha + a_1)\,\alpha + a_0 (opravdo$$

a hodnotu $p(\alpha)$ počítat postupně vyhodnocováním závorek od vnitřní k vn
Snadno zjistíme (roznásobením závorek), že oba vzorce dávají skutečně t
hodnotu $p(\alpha)$, ovšem vzorec (??) je daleko méně numericky náročný. P
stavme si, že stupeň polynomu je 1524. Podle vzorce (??) bychom museli poč
nejprve mocninu α^{1524}, zatímco vzorec (??) nás do ničeho takového nenut

Programátorští amatéři (kteří bohužel často fušují programátorům do
mesla) se poznají například podle toho, že pro vyhodnocení polynomu v b
α použijí vzorec (??) a hloupě argumentují tím, že počítač je rychlý. And
rychlý, ale jakmile bude potřeba vyhodnocovat tisíce polynomů v tisících

uloží do B, atd. K vyhodnocení polynomu stupně n v bodě α stačí prové
násobení a n sčítání.

Bohužel opravdových programátorů je málo, a proto software mnohdy
padá jak vypadá. Uživatel pak nešťastně čeká u svého kompu a nemůže se
čkat výsledku. Hledí do blba, protože na blba, který to naprogramoval, n
možnost se podívat. Často se mu také draze koupený software zhroutí, pro
například postup podle vzorce (??) není numericky stabilní.

Budeme si hrát na pana Hornera, který používal vzorec (??) dávno
tím, než se objevily první počítače a který si zapisoval mezivýsledky do
hledného schématu. Záhy uvidíme, že ty mezivýsledky i ono přehledné sch
se budou hodit.

Označme obsah nejvíce vnitřní závorky ve vzorci (??) symbolem b_{n-2},
sah další závorky označme b_{n-3} a tak dále až konečně poslední závorka (vn
obklopuje výraz označený b_0. K tomu dopišme $b_{n-1} = a_n$. Pro mezivýsle
b_k tedy platí: $b_{n-1} = a_n$, $b_{k-1} = a_k + \alpha b_k$ pro $k = n-1, n-2, \ldots, 3, 2, 1$.
výpočet hodnoty $p(\alpha)$ zapíšeme do třířádkového tzv. *Hornerova schémat*
prvním řádku jsou koeficienty polynomu p a ve třetím řádku zmíněné mez
počty b_i.

$$\begin{array}{c|ccccccc} & a_n & a_{n-1} & a_{n-2} & \ldots & a_2 & a_1 & a_0 \\ \alpha: & & \alpha b_{n-1} & \alpha b_{n-2} & \ldots & \alpha b_2 & \alpha b_1 & \alpha b_0 \\ \hline & b_{n-1} & b_{n-2} & b_{n-3} & \ldots & b_1 & b_0 & p(\alpha) \end{array}$$

Schéma v druhém a třetím řádku plníme postupně zleva doprava tak, že do
hého řádku šikmo přepisujeme hodnotu třetího řádku násobenou α a násle
směrem dolů sčítáme.

[horner1] Najdeme hodnotu polynomu $2x^8 - 3x^7 - 11x^6 + 5x^5 + 11x$
$2x^2 - 9x - 2$ v bodě 3 za použití Hornerova schématu.

$$\begin{array}{cccccccccc} & 2 & -3 & -11 & 5 & 0 & 11 & -2 & -9 & -2 \\ x = 3: & & 6 & 9 & -6 & -3 & -9 & 6 & 12 & 9 \end{array}$$

a píšeme do druhého řádku následujícího sloupce: 6. Ve sloupci sčítáme. stáváme 3. Tuto trojku násobíme znovu hodnotou $x = 3$ a výsledek 9 píš do druhého řádku následujícího sloupce. Sčítáme, násobíme, sčítáme, násob atd. až nakonec dospíváme k číslu 7, což je hodnota daného polynomu v b $x = 3$.

[horner3] Mezivýsledky b_i z Hornerova schématu jsou koeficienty čás ného podílu polynomu p při dělení polynomem daným vzorcem $x - \alpha$. Zby 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 $a_k = b_{k-1} - \alpha b_k$) $k = n-1, n-2, \ldots, 3, 2, 1$. Podle posledního sloupce Hornerova schémat $a_0 + \alpha b_0 = p(\alpha)$, neboli $a_0 = p(\alpha) - \alpha b_0$. Tyto skutečnosti dosadíme do vz pro výpočet hodnoty polynomu p v bodě $x \in \mathbf{R}$:

$$
\begin{aligned}
p(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = \\
&= b_{n-1} x^n + (b_{n-2} - \alpha b_{n-1})\, x^{n-1} + \cdots + (b_1 - \alpha b_2) x^2 + (b_0 - \alpha b_1)\, x \\
&= x\,(b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \cdots + b_1 x + b_0) - \alpha\,(b_{n-1} x^{n-1} + \cdots + b_2 \\
&= (b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \cdots + b_2 x^2 + b_1 x + b_0)\,(x - \alpha) + p(\alpha).
\end{aligned}
$$

Najdeme částečný podíl a zbytek při dělení polynomu z příkladu ?? p nomem $x - 3$. Podle předchozí věty je

$$
\frac{2x^8 - 3x^7 - 11x^6 + 5x^5 + 11x^3 - 2x^2 - 9x - 2}{x - 3} = 2x^7 + 3x^6 - 2x^5 - x^4 - 3x^3
$$

Koeficienty částečného podílu jsme opsali z třetího řádku Hornerova schém v příkladu ??. Toto je zřejmě méně pracná metoda hledání částečného po než metoda popsaná v důkazu věty ??. Bohužel se tato metoda dá použít jen

Místo reálných čísel ale můžeme používat jakýkoli číselný obor, ve kte umíme čísla mezi sebou sčítat, odčítat, násobit a dělit (podle jistých vlastno podrobněji si o tom povíme v kapitole patnácté). Pokud budeme za poly považovat komplexní funkci komplexní proměnné danou vzorečkem (??), ve rém jsou koeficienty $a_0, a_1, \ldots, a_n$ komplexní čísla a za proměnou x dosazuj komplexní čísla, mluvíme o *polynomu nad* **C**.

Pokud zaměníme slovo „reálný" slovem „komplexní" a symbol **R** sym lem **C** v celém předchozím textu v této kapitole, všechna tvrzení zůstáva platnosti. Budeme-li v následujícím textu v této kapitole mluvit o polynom a nespecifikujeme číselný obor, budeme předpokládat polynomy nad **C**. J z toho důvodu, že budeme vyšetřovat vlastnosti kořenů polynomů. Reálné řeny polynomů nad **R** přitom nemusejí existovat.

[dkoren] *Kořen polynomu* p je takové číslo $\alpha \in \mathbf{C}$, pro které je $p(\alpha)$ Pokud α je kořen polynomu p, pak polynom daný vzorcem $x - \alpha$ pro všec $x \in \mathbf{C}$ nazýváme *kořenový činitel polynomu* p.

[korencdeli] Polynom p je dělitelný svým kořenovým činitelem.

Důkaz. Zbytek po dělení polynomu p polynomem $x-\alpha$ má podle věty ?? stu menší než 1, tedy jedná se o konstantu. Označme ji c. Pro všechna $x \in \mathbf{C}$ p $p(x) = r(x)\,(x - \alpha) + c$. Po dosazení $x = \alpha$ máme $p(\alpha) = r(\alpha) \cdot 0 + c$ Protože α je kořen, je $p(\alpha) = 0$, takže $c = 0$. Skutečně tedy polynom $x - \alpha$ polynom p beze zbytku.

[prozklad] Nechť α_1 je kořen nenulového polynomu p. Zatím ponech stranou problém hledání kořene a spokojíme se s tím, že kořen polynom existuje a označíme jej α_1. Podle předchozí věty je možné dělit kořeno činitelem, neboli $p(x) = r_1(x)\,(x-\alpha_1)$. Z této rovnosti plyne, že všechny ko polynomu r_1 jsou zároveň kořeny polynomu p. Polynom p má kromě ko polynomu r_1 navíc jen kořen α_1. Je tedy možné hledat další kořeny polyn máme

$$p(x) = r_m(x)\,(x-\alpha_1)\,(x-\alpha_2)\cdots(x-\alpha_m), (rozkladp)$$

kde r_m je polynom bez kořenů (věta ?? ukáže, že takový případ nastává
pro konstatní polynom) a α_i jsou všechny kořeny polynomu p. V zápise
se mohou některé kořeny α_i vyskytovat vícekrát. Takovým kořenům řík
vícenásobné, viz následující definice.

[dnasobnost] Kořen α nenulového polynomu p nazýváme k-násobný,
kud polynom $(x-\alpha)^k$ dělí polynom p, a přitom polynom $(x-\alpha)^{k+1}$ ne
polynom p. Občas je užitečné mluvit také o číslu α jako o 0-násobném ko
polynomu p tehdy, když číslo α není kořenem polynomu p.

[nasobnostk] Nenulový polynom p má kořen α násobnosti k právě te
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 poly
q tak, že $p(x) = (x-\alpha)^k q(x)$ pro všechna $x \in \mathbf{C}$, stačí podle definic
dokázat, že $(x-\alpha)^{k+1}$ nedělí p právě když $q(\alpha) \neq 0$, neboli $(x-\alpha)^{k+1}$
p právě když $q(\alpha) = 0$. Nechť $(x-\alpha)^{k+1}$ dělí p, tedy existuje polyno
tak, že $p(x) = (x-\alpha)^k(x-\alpha)\,r(x)$. Z jednoznačnosti podílu je zřejmé
musí $q(x) = (x-\alpha)\,r(x)$, takže $q(\alpha) = 0$. Obráceně, pokud $q(\alpha) = 0$,
podle věty ?? existuje polynom r tak, že $q(x) = (x-\alpha)\,r(x)$. Z toho plyne
$p(x) = (x-\alpha)^k(x-\alpha)\,r(x)$, neboli $(x-\alpha)^{k+1}$ dělí p.

[nasobnost2] Dejme tomu, že víme, že polynom $x^6 - 5x^5 - 15x^4 + 85$
$10x^2 - 372x + 360$ má kořen 2. Určíme násobnost tohoto kořene.

tem až do doby, než polynom r_i nebude mít kořen dvojku.

$$
\begin{array}{rrrrrrrr}
 & 1 & -5 & -15 & 85 & 10 & -372 & 360 \\
2: & & 2 & -6 & -42 & 86 & 192 & -360 \\
\hline
 & 1 & -3 & -21 & 43 & 96 & -180 & 0 \\
2: & & 2 & -2 & -46 & -6 & 180 & \\
\hline
 & 1 & -1 & -23 & -3 & 90 & 0 & \\
2: & & 2 & 2 & -42 & -90 & & \\
\hline
 & 1 & 1 & -21 & -45 & 0 & & \\
2: & & 2 & 6 & -30 & & & \\
\hline
 & 1 & 3 & -15 & -75 & & &
\end{array}
$$

Vidíme tedy, že $p(x) = (x^3 + x^2 - 21x - 45)(x - 2)^3$. Přitom hodnota polyn
$x^3+x^2-21x-45$ pro $x = 2$ je -75, takže dvojka není kořenem tohoto polyno
Číslo 2 je tedy trojnásobný kořen polynomu p.

Násobnost kořene tedy můžeme zjistit opakovaným použitím navazují
Hornerova schématu, přičemž násobnost je počet výsledných řádků konč
nulou s tím, že další řádek už nulou nekončí.

[hledanikorenu] Hledat kořeny polynomu, neboli řešit algebraickou
nici $p(x) = 0$, je úloha důležitá a v praxi často potřebná. Bohužel neexis
obecný postup, jak na základě znalostí koeficientů polynomu $a_0, a_1, \ldots, a_n$
tit přesně kořeny tohoto polynomu. Postupy existují pro velmi speciální
polynomů, například pro polynomy nízkých stupňů. V této poznámce př
meneme, jak je možné hledat kořeny polynomů nízkých stupňů.

−1) Kořeny polynomu stupně -1 (tedy nulového polynomu) jsou všechna k
plexní čísla.

0) Polynom nultého stupně (tedy nenulová konstanta) nemá kořen.

vzorce je možné dohledat v matematických tabulkách (například [3] neb
ovšem pro jejich přílišnou komplikovanost se s nimi člověk často nese
Používají se jen v některých počítačových programech často bez věd
uživatele.

4) Polynom čtvrtého stupně má čtyři kořeny, které lze spočítat z koeficie
polynomu pomocí vzorců, jež je možné dohledat v tabulkách. Ani v to
případě se s těmito vzorci často nesetkáváme.

5) Pro polynomy pátého a vyššího stupně neexistují obecné vzorce pro vy
čet kořenů z koeficientů polynomu. Není pravda, že by v budoucnu ně
tyto vzorce mohl objevit. Niels Abel totiž dokázal, že je to nemožné.

Příroda nám prostřednictvím Abela uštědřila další lekci: poodhalila
své tajemství, které v tomto případě zní: v určitých partiích jsem neodhalite

Je potřeba si uvědomit, že neexistence vzorců pro výpočet kořenů p
nomů stupně pátého a vyššího nemá co dělat s existencí nebo neexistencí
kořenů samotných. Matematik občas pracuje s faktem, že dokáže něčeho e
tenci a současně dokáže, že to co existuje, neumí spočítat. Tak je tomu
tomto případě, jak za chvíli ukáže fundamentální věta algebry ??.

[binomp] Uvažujme tzv. *binomickou rovnici*, tj. rovnici tvaru $x^n - a$
kde $n > 0$ je přirozené číslo a $a \in \mathbf{C}$. Řešení této rovnice jsou všechny ko
polynomu $x^n - a$. To je další speciální typ polynomu, u kterého umíme n
všechny kořeny, dokonce pro libovolný stupeň takového polynomu.

Binomickou rovnici $x^n - a = 0$ přepíšeme do tvaru $x^n = a$ a odmocn
tj. formálně dostáváme $x = \sqrt[n]{a}$. Úkolem je najít všechny n-té odmocni
komplexního čísla a. Toto číslo zapíšeme ve tvaru $a = |a|\,(\cos\alpha + i\sin\alpha)$,
$|a|$ je velikost čísla a a α je úhel v rovině komplexních čísel mezi kladnou reá
osou a polopřímkou s počátkem v bodě 0 procházející bodem a (tzv. *argum*
komplexního čísla a). S využitím Moivreovy věty dostáváme

jsou pro $k \in \{0, 1, 2, \ldots, n-1\}$ různé n-té odmocniny z čísla a. Všechna
čísla řeší danou binomickou rovnici. Ze vzorce (??) plyne, že polynom stu
n má nejvýše n kořenů, takže uvedené n-té odmocniny z čísla a jsou *všec*
kořeny polynomu $x^n - a$.

[fund] Každý polynom stupně aspoň prvého má v $\mathbf{C}$ kořen.

Důkaz. Tato věta je jednoduchým důsledkem složitějších výsledků z kompl
analýzy. Většinou se tedy důkaz věty v prvních semestrech vysokoškolského
dia neuvádí s poukazem na to, že věta bude dokázána později. Z tohoto pohl
se mi líbí důkaz uvedený v [24], který se opírá o relativně jednoduchou m
matiku. Důkaz zde skoro doslova přepisuji včetně některého značení (písm
ξ čteme ksí). Připouštím, že ke čtení potřebuje být čtenář v pohodě a bez
chu. Chci proto naléhavě upozornit, že následující pasáž textu je určena
pro hloubavého čtenáře. Ostatní čtenáři přejdou rovnou k poznámce ??.

V důkazu věty budeme na mnoha místech používat $|xy| = |x|\,|y|$ pro x
$\mathbf{C}$. Tuto vlastnost můžeme ověřit převedením komplexních čísel na tvar
$|x|\,e^{i\alpha}, y = |y|\,e^{i\beta}$ a využitím faktu, že $\left|e^{i(\alpha+\beta)}\right| = 1$ (což plyne z Moivre
věty, viz ??).

Dále často použijeme trojúhelníkovou nerovnost, tedy $|x + y| \le |x|$
pro $x, y \in \mathbf{C}$. Ověříme např. při značení $x = a + ib, y = c + id$. $|x + y|$
$(a + c)^2 + (b + d)^2 = a^2 + b^2 + c^2 + d^2 + 2ac + 2bd$, $(|x| + |y|)^2 = a^2 +$
$2\sqrt{(a^2 + b^2)(c^2 + d^2)} + c^2 + d^2$. Po odečtení a druhém umocnění máme dok
$(ac + bd)^2 \le (a^2 + b^2)(c^2 + d^2)$, což plyne z nerovnosti $0 \le (ad - bc)^2$.

K důkazu fundamentální věty algebry použijeme tři pomocné věty (
mata):

[flemm1] Nechť p je polynom stupně aspoň prvého. Pak $\lim |p(x)| =$
pro $|x| \to +\infty$, neboli $\forall K \ge 0\ \exists r > 0$ tak, že pro všechna $x \in \mathbf{C}$, pro
$|x| > r$, platí $|p(x)| > K$.

Pokud $|x| \to +\infty$, pak $|p(x)| \to +\infty$, protože závorka v posledním výrazu
limitu $|a_n| \neq 0$.

[flemm2] Nechť p je polynom stupně aspoň prvého. Pak funkce $|p| : \mathbf{C}$ -
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
$|p(x)| > K$ pro všechna $x \in \mathbf{C}, |x| > r$. Označme $S_r = \{x \in \mathbf{C}; |x| \leq r\}$
kroužek komplexních čísel o poloměru r se středem 0. Na okraji kroužku
je $|p(x)| \geq K$, protože $|p|$ je spojitá a vně kroužku má hodnoty větší než
Protože S_r je omezený a kompaktní, dosahuje spojitá funkce $|p|$ na S_r sv
minima. Toto minimum je menší než K, protože $0 \in S_r$ a $|p(0)| = K - 1$. T
minimum leží uvnitř kroužku S_r a jde o lokální minimum funkce $|p|$ na $\mathbf{C}$

[flemm3] Nechť p je polynom stupně aspoň prvého. Nechť číslo $x_0 \in$
zvoleno tak, že $|p(x_0)| > 0$. Potom funkce $|p| : \mathbf{C} \to \mathbf{R}$ nemá lokální minin
v x_0.

Jinými slovy, existuje $\xi \in \mathbf{C}$ (komplexní číslo určující směr, ve kterém
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 p
pokladu o stupni p nenulový. Číslo x_0 je kořenem polynomu $p - c$ a nech
je násobnost x_0. Je $m \geq 1$ a podle věty ?? polynom $(x - x_0)^m$ dělí poly
$p - c$, neboli existuje nenulový polynom q tak, že $p(x) - c = (x - x_0)^m q(x)$
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
odmocninu z komplexního čísla $-\frac{c}{d}$, viz příklad ??. Je tedy $\xi^m \frac{d}{c} = -1$.

Pro $t \in \mathbf{R}$ počítejme $p(x_0 + t\xi)$:

$$p(x_0+t\xi) = c+(t\xi)^m q(x_0+t\xi) = c+(t\xi)^m \big(q(x_0+t\xi)-d+d\big) = c+t^m\xi^m d+t^m$$

$|t|(|b_1|+\cdots+|b_s|\,t^{s-1}) \leq |t|(|b_1|+\cdots+|b_s|)$, takže stačí volit $K = |b_1|+\cdots+$
Vraťme se k počítání $p(x_0 + t\xi)$. Využijeme rovnost $\xi^m \frac{d}{c} = -1$.

$$p(x_0+t\xi) = c+t^m\xi^m d+t^m\xi^m r(t) = c\left(1 + t^m\xi^m\frac{d}{c} + t^m\xi^m\frac{r(t)}{c}\right) = c\left(1 -\right.$$

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
novaná absolutní hodnota je menší než 1 pro malá kladná t. Využijeme od
$|r(t)| \leq Kt$:

$$\left|1 - t^m + t^m\xi^m\frac{r(t)}{c}\right| \leq |1 - t^m|+\left|t^m\xi^m\frac{Kt}{c}\right| = 1-t^m+t^{m+1}K\left|\frac{\xi^m}{c}\right| = 1+t^m$$

Pro dostatečně malá $t > 0$ je poslední závorka blízká číslu -1, tedy zápo
takže uvedený výraz jako celek je menší než 1.

Důkaz fundamentální věty algebry ??. Podle věty ?? funkce $|p|: \mathbf{C}$ –
nabývá svého lokálního minima. Podle věty ?? toto minimum není v bodě
kterém $|p(x)| > 0$. Protože $|p(x)| \geq 0$, musí být hledané minimum v b
$x \in \mathbf{C}$, pro které je $|p(x)| = 0$, tj. $p(x) = 0$. Existence kořenu je dokázána.

[poznrozklad] Důsledkem věty ?? je skutečnost, že polynom r_m ve vzorc
je konstantní. Z toho a z věty ?? také plyne, že polynom p má ve vzorci (??)
kořenových činitelů, kolik je jeho stupeň. Počítáme-li tedy každý kořen tolik
kolik je jeho násobnost, můžeme říci, že polynom má stejný počet kořenů,
je jeho stupeň. Konečně, protože $(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_m) = 1x^m +$
musí být konstantní polynom r_m roven koeficientu a_m, což je nenulový koe
ent u nejvyšší mocniny polynomu p. Všechny tyto poznatky zformulujeme
následující věty.

[komplrozklad] Nechť p je nenulový polynom stupně n s koeficienty a_0, a

Důkaz. Viz poznámku ??.

[maxkorenup] Nenulový polynom stupně n má nejvýše n různých komp
ních kořenů.

Důkaz. Věta je přímým důsledkem věty ??.

Pokud se dva polynomy stupně nejvýše n shodují v $n+1$ různých bod
pak jsou totožné. Jinými slovy, polynom stupně n je jednoznačně určen sv
hodnotami v $n+1$ bodech.

Důkaz. Předpokládáme, že pro polynomy p a q existují vzájemně různá
$\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1}$ taková, že $p(\alpha_i) = q(\alpha_i)$ pro $i \in \{1, 2, \ldots, n, n+1\}$. Pro
polynomy p a q mají stupeň nejvýše n, je podle věty ?? rozdíl $p - q$ poly
stupně nejvýše n, který má kořeny $\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1}$. Těch kořenů je
než je jeho stupeň. To podle věty ?? není možné jinak, než že je polynom
nulový. Takže $p = q$ a důkaz je hotov.

Bude následovat několik modelových příkladů na rozklad polynomu na
řenové činitele. Je potřeba si uvědomit, že tyto příklady jsou schválně vo
tak, aby se povedlo kořeny uhádnout. Poznámka ?? ale mluví jasně: moc
ností při hledání kořenů nemáme. Modelové příklady na hledání kořenů
často typické tím, že se dá uhádnout kořen jako malé celé číslo nebo jedno
chý zlomek. Abychom mohli hádat jen z konečně mnoha možností, využij
následující dvě věty.

[delia0] Nechť polynom p má celočíselné koeficienty $a_0, a_1, \ldots, a_n$. Je-
celočíselným kořenem polynomu p, pak α dělí koeficient a_0.

Důkaz. Věta je speciálním případem následující věty pro $d = 1$.

[delirac] Nechť polynom p stupně n má celočíselné koeficienty $a_0, a_1, \ldots$
Je-li $\alpha = \frac{c}{d}$ racionálním kořenem polynomu p a čísla c, d jsou celá nesoudě

Po převedení a_0 na druhou stranu rovnosti, vynásobení rovnosti číslem c
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, k
označíme k. Výše uvedená rovnost má tvar $c \cdot k = a_0 \cdot e$. Číslo c tedy musí
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

[polyn360] 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
Bohužel dělitelů čísla 360 je mnoho. Čtenář si za domácí cvičení zkusí všec
dělitele vypsat. Shledá, že jich je 48, pokud ovšem nezapomene zapsat i zápo
dělitele. Obvykle začínáme dosazovat takové dělitele, které jsou v absol
hodnotě co nejmenší. Tedy $p(1) = 64$ (není kořen), $p(-1) = 648$ (není koř
$p(2) = 0$ (ejhle, je to kořen)! Navíc, jak ukazuje příklad ??, je tento ko
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 $x^3 + x^2 - 21x -$
Dále tedy hledáme kořeny jen tohoto kubického polynomu r. Hádáme dále
čísla (protože v modelových příkladech nás nikdo nebude nutit použít C
danovy vzorce). Stačí se omezit na dělitele čísla 45, tedy na čísla z mno
$\{-45, -15, -9, -5, -3, -1, 1, 3, 5, 9, 15, 45\}$. Jedničku a mínus jedničku už j
testovali s negativím výsledkem v případě polynomu p, nemusíme ji tedy z
šet znovu. Vyzkoušíme $r(3) = -72$ (není kořen), $r(-3) = 0$ (ejhle koř
Hornerovo schéma pro -3 vypadá takto:

Vidíme, že číslo -3 je dvojnásobný kořen a že je $x^3 + x^2 - 21x - 45 = ($
$3)^2(x-5)$, takže 5 je poslední kořen vyšetřovaného polynomu. Máme rozk

$$x^6 - 5x^5 - 15x^4 + 85x^3 + 10x^2 - 372x + 360 = (x-2)^3(x+3)^2(x-5)$$

Polynom p má tedy následující kořeny: 2 (trojnásobný kořen), -3 (dvojnáso kořen) a 5 (jednonásobný kořen).

[polyn26] Najdeme rozklad polynomu $3x^6 - 8x^5 + 22x^4 + 54x^3 - 5x^2 -$ na kořenové činitele.

Označme vyšetřovaný polynom písmenem p. Především, tento poly má koeficient $a_0 = 0$, takže nula je kořenem polynomu. Kořenový činitel x píšeme stručně jako x a vznikne jednoduše vytknutím proměnné x ze zada výrazu:

$$p(x) = x\,(3x^5 - 8x^4 + 22x^3 + 54x^2 - 5x - 26).$$

Dále stačí najít rozklad polynomu $3x^5 - 8x^4 + 22x^3 + 54x^2 - 5x - 26$, k označíme q. Nejprve hádáme celočíselné kořeny mezi děliteli čísla 26: $q(1) =$ (není kořen), $q(-1) = 0$ (ejhle, kořen)! Navazujícím Hornerovým schéma vyzkoumáme jeho násobnost:

$$\begin{array}{r|rrrrrr}
 & 3 & -8 & 22 & 54 & -5 & -26 \\
-1: & & -3 & 11 & -33 & -21 & 26 \\
\hline
 & 3 & -11 & 33 & 21 & -26 & 0 \\
-1: & & -3 & 14 & -47 & 26 & \\
\hline
 & 3 & -14 & 47 & -26 & 0 & \\
-1: & & -3 & 17 & -64 & & \\
\hline
 & 3 & -17 & 64 & -90 & &
\end{array}$$

Číslo -1 je tedy dvojnásobným kořenem a máme $q(x) = (x+1)^2(3x^3 - 14$

26 a jmenovatel dělí 3. Vyzkoušíme $r(1/3) \doteq -11{,}777$ (není kořen), $r(-1/3$
$-43{,}333$ (není kořen), $r(2/3) = 0$ (ejhle kořen)! Pomocí Hornerova schém
můžeme najít rozklad:

$$\begin{array}{r|rrrr} & 3 & -14 & 47 & -26 \\ 2/3: & & 2 & -8 & 26 \\ \hline & 3 & -12 & 39 & 0 \end{array}$$

Takže $r(x) = (x - \frac{2}{3})(3x^2 - 12x + 39)$. Kořeny kvadratického polynomu um
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 koefic
u nejvyšší mocniny a_6 polynomu p. Na něj nesmíme zapomenout. Polyno
má nulu jako jednonásobný kořen, -1 je dvojnásobný kořen, $\frac{2}{3}$ je jedn
sobný kořen a konečně čísla $2 + 3i$ a $2 - 3i$ jsou vzájemně komplexně sdru
jednonásobné kořeny.

[nenajdukoreny] Pokusíme se najít rozklad na kořenové činitele polyn
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 či
musí dělit dvojku a jmenovatel musí také dělit dvojku. Kořeny budeme t

o komplexní kořeny s nenulovou imaginární částí. Bohužel, ani jeden tak kořen neumíme najít, ačkoli koeficienty toho polynomu vypadají celkem nev (jsou to malá celá čísla). Můžeme tedy pouze prohlásit, že rozklad na kořer činitele tohoto polynomu existuje, ale nevíme, jak tento rozklad vypadá.

Chtěl bych velmi upozornit, že toto je obvyklý jev. Pokud náhodně v reme z osudí, ve kterém jsou všechny polynomy, jeden, pak skoro jistě neum najít jeho kořeny. Desítky, možná stovky, příkladů, které se vyskytují v u nicích základního kurzu o polynomech, jsou vyumělkované a voleny tak, bylo možné nějak kořeny najít. Daleko typičtější je ovšem příklad tento: ko najít neumíme.

V praxi se můžeme setkat navíc s polynomy vysokých stupňů, jejichž ficienty ani nejsou celá čísla. Pak si můžeme být skoro jisti, že kořeny n nelze. Protože ale úloha rozkladu na kořenové činitele a hledání kořenů je další výpočty většinou potřebná, je nutné přistoupit k hledání kořenů ales přibližně numerickými metodami. Tato problematika ale nespadá do ná tohoto textu.

Pro ilustraci jsem použil řešítko v Maple, které má v sobě zabudov numerické metody hledání kořenů. Pro daný polynom vyšel tento přibl výsledek:

$$
\begin{aligned}
&x_1 \doteq -2{,}05376, \quad x_2 \doteq -0{,}55262, \quad x_3 \doteq -0{,}25957, \quad x_4 \doteq 2{,}99882,\\
&x_{5,6} \doteq -0{,}26936 \pm 1{,}00279\, i, \quad x_{7,8} \doteq 0{,}95292 \pm 0{,}37662\, i,\\
&p(x) = 2\,(x-x_1)\,(x-x_2)\,(x-x_3)\,(x-x_4)\,(x-x_5)\,(x-x_6)\,(x-x_7)\,(x-
\end{aligned}
$$

Najdeme rozklad polynomu $x^n - a$ na kořenové činitele.

Využijeme výsledku příkladu ??. Rozklad na kořenové činitele je

$$x^n - a = \prod_{k=0}^{n-1} \left(x - \sqrt[n]{|a|} \left(\cos \frac{\alpha + 2k\pi}{n} + i \sin \frac{\alpha + 2k\pi}{n} \right) \right), (birozklad)$$

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 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 konc pro $k = 4$ je $\sqrt[8]{1} = -1$. Z tohoto hlediska je nutno tento příklad považ za modelový, neboť potřebné hodnoty funkcí sinus a kosinus byly tabulk Kdybychom počítali např. $\sqrt[7]{1}$, tabulkových hodnot bychom nemohli vy a museli bychom nechat výsledek ve tvaru (??) nebo jej vyčíslit numeri Rozklad polynomu $x^8 - 1$ na kořenové činitele je

$$x^8-1 = \left(x-1\right)\left(x-\tfrac{\sqrt{2}}{2}-i\tfrac{\sqrt{2}}{2}\right)\left(x-\tfrac{\sqrt{2}}{2}+i\tfrac{\sqrt{2}}{2}\right)\left(x-i\right)\left(x+i\right)\left(x+\tfrac{\sqrt{2}}{2}-i\tfrac{\sqrt{2}}{2}\right)\left(x+\right.$$

V příkladech ??, ??, ?? vyšly komplexní kořeny vzájemně po dvou k plexně sdružené. Následující věty ukazují, že se nejedná o náhodu, ale polynomy s reálnými koeficienty je to zákonitá vlastnost.

[alphaspruhem] Je-li α kořen polynomu p s reálnými koeficienty, pak k plexně sdružené číslo $\overline{\alpha}$ je také kořenem polynomu p.

Důkaz. Připomenu, že komplexně sdružené číslo značíme pruhem nad čís a definujeme jako číslo s opačnou imaginární částí, tj. $\overline{a+ib} = a - ib$. Dá 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 $\overline{a+ib} + \overline{c+id} = a + c - i(b+d) = \overline{a+ib+c}$
$\overline{x}\,\overline{y} = \overline{xy}$, protože $(a-ib)(c-id) = ac-bd-i(bc+ad) = \overline{ac-bd+i(bc+}$ $\overline{(a+ib)(c+id)}$.
$\overline{x^n} = \overline{x}^n$, 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 $p(\overline{\alpha}) = 0$.

$$p(\overline{\alpha}) = a_0 + a_1\overline{\alpha} + a_2\overline{\alpha}^2 + \cdots + a_n\overline{\alpha}^n = \overline{a_0} + \overline{a_1}\ \overline{\alpha} + \overline{a_2}\ \overline{\alpha}^2 + \cdots + \overline{a_n}\ \overline{\alpha}^n$$

$$= \overline{a_0} + \overline{a_1}\ \overline{\alpha} + \overline{a_2}\ \overline{\alpha^2} + \cdots + \overline{a_n}\ \overline{\alpha^n} = \overline{a_0} + \overline{a_1\alpha} + \overline{a_2\alpha^2} + \cdots + \overline{a_n\alpha^n}$$

[nasobnostpruhu] Nechť α je kořen nenulového polynomu p s reálnými ficienty. Pak kořeny α a $\overline{\alpha}$ mají stejnou násobnost.

Důkaz. Předpokládejme, že násobnost kořene α je k a násobnost $\overline{\alpha}$ je k'. újmy na obecnosti je možno předpokládat $k \leq k'$. V rozkladu na kořen činitele polynomu p se vyskytuje kromě $(x - \alpha)$ také činitel $(x - \overline{\alpha})$. So 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 re koeficienty a navíc dělí polynom p beze zbytku. Označme $p/q = r$. Polyno má (díky algoritmu pro dělení polynomu polynomem) reálné koeficienty. může se tedy stát, aby r měl jen kořen $\overline{\alpha}$, a přitom neměl kořen α. Násobn tedy musejí být stejné.

[realrozklad] Pokud je dán polynom s reálnými koeficienty, pak podle p chozí věty má stejný počet kořenových činitelů tvaru $x - \alpha$ jako činitelů t $x - \overline{\alpha}$. Tyto činitele můžeme po dvou roznásobit a vytvořit tak kvadrat polynomy s reálnými koeficienty

$$(x - \alpha)\,(x - \overline{\alpha}) = (x - a - ib)\,(x - a + ib) = x^2 - 2ax + a^2 + b^2 = x^2 + cx$$

Tím se v rozkladu na součin polynomů vyhneme práci s komplexními čísly může být pro uživatele, který pracuje s reálnými polynomy a očekává tedy álné rozklady, důležité. Zformulujeme proto větu o reálném rozkladu na so polynomů.

[rrozkladp] Nechť nenulový polynom p stupně n má reálné koeficie Nechť $\alpha_1, \alpha_2, \ldots, \alpha_s$ jsou všechny jeho vzájemně různé reálné kořeny s ná nostmi po řadě $k_1, k_2, \ldots, k_s$. Nechť $\beta_1, \overline{\beta_1}, \ldots, \beta_t, \overline{\beta_t}$ jsou všechny vzáje různé komplexní kořeny polynomu p s nenulovou imaginární částí, které

Uvedený vzorec se nazývá *reálný rozklad polynomu p*.

Důkaz. Je $(x-\beta_i)(x-\overline{\beta_i}) = x^2 + c_i x + d_i$, viz poznámku ??. Vše ostatní p
z věty ??.

Rozklad na kořenové činitele v příkladu ?? je současně reálným rozklad
protože polynom nemá komplexní kořeny s nenulovou imaginární částí.

Polynom z příkladu ?? má reálný rozklad $p(x) = 3x\,(x+1)^2(x-\frac{2}{3})\,($
$4x+13)$.

Polynom z příkladu ?? má reálný rozklad $p(x) = (x-1)\,(x+1)\,($
$1)\,(x^2+\sqrt{2}\,x+1)\,(x^2-\sqrt{2}\,x+1)$.

Konečně polynom z příkladu ?? má reálný rozklad přibližně:

$p(x) \doteq 2\,(x-x_1)\,(x-x_2)\,(x-x_3)\,(x-x_4)\,(x^2+0{,}53872\,x+1{,}07814)\,($
$1{,}90584\,x+1{,}0499)$.

Rozložíme polynom $x^5-10x^4+32x^3-8x^2-140x+200$ na reálné kořen
činitele. Využijeme přitom nápovědy, že číslo $3+i$ je kořenem tohoto polyno

Především je zřejmé, že se jedná o modelový příklad. Je totiž nereá
aby nám v reálném životě někdo napovídal nereálný kořen reálného polyno

Protože má polynom reálné koeficienty, je podle věty ?? také číslo 3
kořenem. Známe tedy dva kořeny. Nyní máme dvě možnosti, jak dále po
povat. Můžeme například pomocí Hornerova schématu dosadit jednak $3+$
následně $3-i$ do polynomu. Druhou možností je roznásobit kořenové čin
příslušející známým kořenům a podělit výsledným kvadratickým polynom
daný polynom. Vyzkoušíme si obě metody.

Nejprve zkusíme dosazovat kořeny do Hornerova schématu. Zpočátk
půjde ztuha, protože člověk nenásobí dvě komplexní čísla mezi sebou denn

	1	-10	32	-8	-140	2
$3+i:$		$3+i$	$-22-4i$	$34-2i$	$80+20i$	-2

Jak jsme ukázali v důkazu věty ??, polynom r má reálné koeficienty. Je t
$p(x) = (x-3-i)\,(x-3+i)\,(x^3-4x^2-2x+20)$.

Než začneme rozkládat polynom r, zkusíme se ke stejnému mezivýsle
dostat druhou metodou. Roznásobíme nejdříve kořenové činitele $(x-3-i)$
$3+i) = x^2-6x+10$. Tím jsme se hned na začátku zbavili malého měkkéh
Abychom získali polynom r, musíme bohužel dělit polynom p polynomem
$6x+10$.

$$
\begin{array}{rl}
(x^5-10x^4+32x^3-\;\;8x^2-140x+200) & :(x^2-6x+10) = x^3-4x^2-2x \\
-(x^5-\;\;6x^4+10x^3) & \\
\hline
-4x^4+22x^3-\;\;8x^2-140x+200 & \\
-(-4x^4+24x^3-40x^2) & \\
\hline
-2x^3+32x^2-140x+200 & \\
-(-2x^3+12x^2-\;\;20x) & \\
\hline
20x^2-120x+200 & \\
-(20x^2-120x+200) & \\
\hline
0 &
\end{array}
$$

Ne náhodou vyšel zbytek po dělení nula. Polynom $x^2-6x+10$ musí
polynom p, protože se jedná o součin kořenových činitelů.

Nyní se nám obě metody setkávají. Potřebujeme rozložit polynom
kořenové činitele. Hádáme mezi děliteli čísla 20: $r(1) = 15$ (není kořen), $r(-$
17 (není kořen), $r(2) = 8$ (není kořen), $r(-2) = 0$ (ejhle kořen)! Po vydě
kořenovým činitelem $x+2$ (nebo použitím Hornerova schématu) dostáv
$r(x) = (x+2)\,(x^2-6+10)$. Protože polynom x^2-6+10 už v rozkladu jed
máme, shledáváme, že kořeny $3\pm i$ jsou dvojnásobné. Reálný rozklad polyn
p tedy je

$$p(x) = (x+2)\,(x^2-6+10)^2.$$

dále možno rozepsat na součet parciálních zlomků, jak uvidíme v násled větě ??. Nejprve ovšem potřebujeme dokázat pomocnou větu:

[parczlpom] Nechť stupeň polynomu p je menší než stupeň polynom a nechť $\alpha \in \mathbf{C}$ je k-násobným kořenem polynomu q. Symbolem q_1 ozna polynom, který splňuje $q(x) = (x-\alpha)^k q_1(x)$ pro všechna $x \in \mathbf{C}$. Pak exis 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 m než stupeň $(x-\alpha)^{k-1} q_1(x)$.

Důkaz. Vynásobením dokazované rovnosti polynomem q dostaneme ekv lentní rovnost:

$$p(x) = a\, q_1(x) + p_1(x)\,(x-\alpha).$$

Dosazením $x = \alpha$ dostáváme $p(\alpha) = a\, q_1(\alpha)$, tedy $a = p(\alpha)/q_1(\alpha)$. T 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 $p(\alpha) - \big(p(\alpha)/q_1(\alpha)\big)\, q_1($ 0. Existuje tedy podle věty ?? polynom p_1 tak, že $p(x) - a\, q_1(x) = p_1(x)\,(x-$ Přičtením $a\, q_1(x)$ a vydělením polynomem q dostáváme dokazovanou rovn

Protože $\mathrm{St}(p_1) + 1 \le \max\big(\mathrm{St}(p), \mathrm{St}(q_1)\big) < \mathrm{St}(q)$, je $\mathrm{St}(p_1) < \mathrm{St}(q)$ Takže platí i tvrzení o stupni polynomu p_1.

[parczl2] Nechť stupeň polynomu p je menší než stupeň polynomu nechť α je k-násobným kořenem polynomu q. Symbolem q_1 označme polyn který splňuje $q(x) = (x-\alpha)^k q_1(x)$ pro všechna $x \in \mathbf{C}$. Pak existují $a_1, a_2, \ldots, a_k \in \mathbf{C}$ a polynom p_2 tak, že platí:

[parczl] Podíl polynomů p/q, kde stupeň p je menší než stupeň q, je ro
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 $u \le k$, $u \in \mathbf{N}$.

Důkaz. Použijeme větu ?? postupně na všechny kořeny polynomu q.

Důkazy vět ?? a ?? jsou konstruktivní, tj. poskytují návod, jak spoč
konstanty, které se vyskytují v čitatelích všech parciálních zlomků. Čtená
měl umět po pečlivém přečtení těchto důkazů implementovat algoritmus, k
pro každé dva polynomy p a q (stupeň p je menší než stupeň q a u polyno
q jsou známy kořeny) sestaví součet parciálních zlomků.

V kurzech kalkulu jedné proměné se při integrování lomených funkcí
funkcí ve tvaru podílu polynomů) pracuje s vybranými příklady, ve kterýc
podaří najít kořeny jmenovatele. Je třeba si ale uvědomit, že pokud se nepo
kořeny jmenovatele přesně najít (což je u polynomů stupně pátého a vyš
obvyklé), pak nelze přesně sestavit ani parciální zlomky a integrovat můž
jen „teoreticky“.

Abychom se při integraci vyhnuli komplexním číslům, rozepisují se po
polynomů s reálnými koeficienty na součet parciálních zlomků dvou druhů. V
o součtu *reálných* parciálních zlomků má tvar:

[parczlrell] Podíl polynomů p/q, kde stupeň p je menší než stupeň q a
mají reálné koeficienty, je roven součtu konečně mnoha tzv. *parciálních zlo*
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

[parczlrel] Nechť p a q jsou polynomy s reálnými koeficienty a nechť stu
p je menší než stupeň q. Předpokládejme, že $\beta \in \mathbf{C}$, $\beta \notin \mathbf{R}$ je k-násob
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 $b \in \mathbf{R}$, $c \in$
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 polyn
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 ekv
lentní 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 $b\,\beta +$
$p(\beta)/q_1(\beta)$. Tento výpočet lze provést, protože díky větám ?? a ?? je $q_1(\beta)$

Označme $\beta = u + iv$ a $p(\beta)/q_1(\beta) = t + is$, kde $u, v, t, s \in \mathbf{R}$. Je $b($
$iv) + c = t + is$, takže $b = s/v$ a $c = t - (s/v)\,u$. Z výpočtu plyne, že čísla
existují a jsou reálná.

Polynom $p(x) - (bx+c)\,q_1(x)$ má kořen $\beta \in \mathbf{C}$, protože $p(\beta) - \big(p(\beta)/q_1(\beta$
0. Tento polynom má také kořen $\overline{\beta}$, protože má reálné koeficienty a p
věta ??. Existuje tedy podle věty ?? polynom p_1 s reálnými koeficienty
že $p(x) - (bx+c)\,q_1(x) = p_1(x)\,(x-\beta)(x-\overline{\beta})$. Přičtením $(bx+c)\,q_1($
vydělením polynomem q dostáváme dokazovanou rovnost.

Protože $\mathrm{St}(p_1) + 2 \le \max\big(\mathrm{St}(p), \mathrm{St}(q_1)+1\big) < \mathrm{St}(q)$, je $\mathrm{St}(p_1) < \mathrm{St}(q)$
Takže platí i tvrzení o stupni polynomu p

polynomu jsou operace definované v tělese T, pak říkáme, že polynom p je *tělesem T*.

Nechť p je polynom nad tělesem T. Říkáme, že *p je reducibilní v T*, po existují polynomy q, r stupně aspoň prvního nad T tak, že $p = q\,r$. Polyno je *ireducibilní v T*, jestliže není reducibilní v T.

Slovo *ireducibilní* můžeme přeložit jako *nerozložitelný* na součin polyn nižšího stupně v číselném oboru koeficientů, který je stanoven tělesem T. příklad polynom $x^2 + 1$ je ireducibilní v $\mathbf{R}$, ale není ireducibilní v $\mathbf{C}$, pro $x^2 + 1 = (x - i)(x + i)$.

Z definice je zřejmé, že konstantní polynomy a polynomy stupně prv jsou určitě ireducibilní v libovolném tělese, protože podle věty ?? nemo existovat dva polynomy stupně aspoň prvního, jejichž součin je polynom stu nejvýše prvního.

Z fundamentální věty algebry plyne tento důležitý poznatek: *ireduci polynomy v $\mathbf{C}$ jsou pouze polynomy stupně nejvýše prvního*, nebo jinak: *všec polynomy stupně aspoň druhého jsou v $\mathbf{C}$ reducibilní*, nebo ještě jinak: *pro k nenulový polynom existuje rozklad na kořenové činitele, což je rozklad na so ireducibilních polynomů v $\mathbf{C}$*.

Reálný rozklad popsaný ve větě ?? je rozkladem na součin ireducibil polynomů v $\mathbf{R}$. Z této věty plyne, že *ireducibilní polynom v $\mathbf{R}$ má stupeň výše* 2. Ireducibilní polynom $ax^2 + bx + c$ v $\mathbf{R}$ stupně druhého poznáme tak má záporný diskriminant $D = b^2 - 4ac$.

Má-li polynom stupně aspoň druhého nad tělesem T kořen v tělese T, je reducibilní v T. Obrácené tvrzení „nemá-li polynom v tělese T kořen, je ireducibilní v T“ neplatí. Například $(x^2 + 1)^2$ nemá v $\mathbf{R}$ kořen, ale lze rozložit na součin polynomů $(x^2 + 1)\,(x^2 + 1)$ s reálnými koeficienty.

Polynom $x^8 - 1$ z příkladu ?? má rozklad na součin ireducibilních polyno v $\mathbf{C}$:

$$x^8 - 1 = (x - 1)\,\left(x - \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right)\,\left(x - \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)\,(x - i)\,(x + i)\,\left(x + \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right)\,(x +$$

Polynom jsme zavedli jako funkci danou vzorečkem /??/ nebo jako
reček samotný /??/. Definovali jsme součet a skalární násobek těchto
rečků /??/ a ukázali, že tvoří lineární prostor /??/, který je izomorfní s pro
rem polynomů jako funkcí /??/.

Kromě sčítání polynomů a násobení polynomu konstantou umíme p
nomy také násobit mezi sebou /??/ a hledat částečný podíl /??/.

Uvedli jsme si /??/, že Hornerovo schéma umožní nejen efektivně vyhod
covat polynomy ve zvolených bodech α, ale mezivýpočty navíc tvoří koefici
částečného podílu vyhodnocovaného polynomu polynomem $(x - \alpha)$.

Definovali jsme kořen polynomu /??/ a dokázali, že polynom je dělit
svým kořenovým činitelem beze zbytku /??/. Z toho vyplynul rozklad p
nomu na součin kořenových činitelů /??/. Základní věta algebry /??/ zaruč
že tento rozklad lze provést v oboru komplexních čísel. Přitom si musíme
vědomi, že pro obecné polynomy stupně pátého a vyššího vzorce na př
výpočet kořenů z koeficinetů neexistují /??/, takže rozklad je možné psát
teoreticky.

Uvedli jsme si věty /??, ??/, které uvádějí, že v případě celočíselných k
cientů dělí případné celočíselné kořeny koeficient a_0 resp. případný racion
kořen má jistý vztah ke koeficientům a_0 a a_n. Ovšem problém je v tom
polynom s celočíselnými koeficienty nemusí mít žádný racionální kořen (co
navíc typická vlastnost). Pomůže nám to ke hledání kořenů jen pro „mode
příklady".

Věty /??, ??/ říkají, že polynomy s reálnými koeficienty mají své nere
komplexní kořeny v párech vzájemně komplexně sdružené a stejné násobn
To inspiruje k reálnému rozkladu polynomu na součin: stačí snásobit kořen
činitele typu $(x - \alpha)(x - \overline{\alpha})$, což je kvadratický polynom s reálnými koefici
a se záporným diskriminantem.

Krátce jsme zmínili rozklad racionální lomené funkce na parciální zlomk
včetně reálné alternativy /??, ??/.

15. Grupa, těleso

[pteleso] Následující text až do konce kapitoly je poněkud abstrakt
povahy. Přitom se jeho znalost nepředpokládá pro pochopení dalších kap
Pokud tedy čtenář nechce být hned v počátku studia zahlcen pojmy o a
braických strukturách, může tento text přeskočit.

Reálná čísla jsou množina prvků, které umíme vzájemně sčítat a vzáje
násobit. Přesněji, je to množina $\mathbf{R}$, na které jsou definovány obvyklé ope
$+ : \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ a $\cdot : \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ s jistými vlastnostmi (asociativní zákon,
tributivní zákon, atd.). Těmito vlastnostmi se budeme inspirovat a pokus
se vybudovat abstraktní algebraickou strukturu, tzv. *těleso*. Jedním z n
ných konkrétních příkladů tělesa pak samozřejmě budou reálná čísla. Jeno
kromě nich budeme nacházet i jiné příklady těles. Začneme nejprve struktu
s jedinou operací.

[dgrupa] Množinu G, na které je definována operace $\circ : G \times G \to G$ n
váme *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 neut

(3) $\forall x \in G \ \exists y \in G : x \circ y = y \circ x = e$ (existence opačného/inverzního p

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 úc
norskému matematikovi, který rozpracoval teorii grup a bohužel zemřel n
na zákeřnou nemoc ve věku 26 let, se komutativní grupa nazývá též *Abe*
grupa

Množina $\mathbf{R}$ s operací sčítání tvoří grupu. Skutečně platí asociativní zá
pro sčítání reálných čísel: $(x+y)+z = x+(y+z)$, dále existuje neutrální pr
0, pro který $0 + x = x + 0 = x$ a konečně pro každé $x \in \mathbf{R}$ existuje $y =$
tak, že $x + y = y + x = 0$. Navíc se jedná o grupu komutativní, protože sčí
reálných čísel je komutativní.

Pokud operaci grupy značíme symbolem „+“ (jako v tomto příkladě),
obvykle o prvku e z vlastnosti (2) mluvíme jako o neutrálním prvku a znač
ho symbolem „0“ (též nula, nulový prvek) a prvek y z vlastnosti (3) n
vame *opačný* a značíme $-x$. Přičtení opačného prvku v komutativní grupě
nazýváme *odečítání* a místo $a + (-b)$ píšeme $a - b$.

Množina $\mathbf{R} \setminus \{0\}$ s operací násobení tvoří grupu. Skutečně platí asociat
zákon pro násobení reálných čísel: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, dále existuje jednotk
prvek 1, pro který $1 \cdot x = x \cdot 1 = x$ a konečně pro každé $x \in \mathbf{R} \setminus \{0\}$ exis
$y = x^{-1}$ tak, že $x \cdot y = y \cdot x = 1$. Navíc se jedná o grupu komutativní, pro
násobení reálných čísel je komutativní.

Pokud operaci grupy značíme symbolem „·“, pak obvykle prvek e z vl
nosti (2) značíme symbolem „1“ (jedna, jednotkový prvek). Prvek y z vlastn
(3) nazývame *inverzní* a značíme x^{-1}. Násobení inverzním prvkem v kom
tivní grupě nazýváme *dělení* a místo $a \cdot b^{-1}$ píšeme a/b nebo $\frac{a}{b}$.

Množina $\mathbf{R}$ s operací násobení netvoří grupu, protože 0 nemá inve
prvek.

Množina všech reálných funkcí $F = \{f : \mathbf{R} \to \mathbf{R}$, f je prostá a „na
operací *skládání funkcí* $\circ : F \times F \to F$, definovanou pomocí $(g \circ f)(x) = g\big(f$
$\forall x \in \mathbf{R}$, tvoří grupu. Skutečně platí asociativní zákon $(f \circ g) \circ h = f \circ (g \circ$
existuje jednotkový prvek: identické zobrazení i, pro které $i(x) = x$. Ke ka
prosté funkci f lze setrojit funkci inverzní f^{-1} tak, že $f \circ f^{-1} = f^{-1} \circ f$
Přitom se nejedná o grupu komutativní, protože například pro $f(x) =$
$g(x) = 1 + x$ je $(f \circ g)(x) = (1 + x)^3$, zatímco $(g \circ f)(x) = 1 + x^3$.

[gpermutaci] Kdybychom v předchozím příkladě místo funkcí f z $\mathbf{R}$

k tvoří komutativní grupu. Připomínáme, že „x modulo y“ je zbytek při dě
čísla x číslem y. Neutrálním prvkem této grupy je 0 a opačným prvkem k pr
$a \neq 0$ je prvek $k - a$. Samozřejmě, opačným prvkem k prvku neutrálním
prvek neutrální, což ostatně platí v libovolné grupě.

Lineární prostor se svou operací sčítání vektorů (podle definice ??) t
komutativní grupu. Skutečně, asociativní zákon je postulován vlastností
v definici ??, neutrálním prvkem je nulový vektor (viz vlastnost (1) věty ?
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 komutativn

[gdlp] Obráceně, pomocí pojmu grupa můžeme významně zkrátit naši
finici lineárního prostoru ??:

Lineárním prostorem je množina L, která s operací $+ : L \times L \to L$ t
komutativní grupu. Dále musí být na množině L definována operace $\cdot : \mathbf{R} \times$
L, s vlastnostmi $\forall \alpha, \beta \in \mathbf{R}, \forall \boldsymbol{x}, \boldsymbol{y} \in L$:

$$\begin{array}{ll}
\text{(A)} & \alpha \cdot (\beta \cdot \boldsymbol{x}) = (\alpha\beta) \cdot \boldsymbol{x}, \\
\text{(B)} & \alpha \cdot (\boldsymbol{x} + \boldsymbol{y}) = \alpha \cdot \boldsymbol{x} + \alpha \cdot \boldsymbol{y}, \\
\text{(C)} & (\alpha + \beta) \cdot \boldsymbol{x} = \alpha \cdot \boldsymbol{x} + \beta \cdot \boldsymbol{x}, \\
\text{(D)} & 1 \cdot \boldsymbol{x} = \boldsymbol{x}.
\end{array}$$

Vzhledem k tomu, že vlastnosti (1), (2) definice ?? přímo korespondu
vlastnostmi komutativní grupy, stačí ověřit, že nám z této nové definice vyp
vlastnost (7) definice ??, která jediná zde chybí. Existence nulového vektor
zajištěna jako existence neutrálního prvku $\boldsymbol{o}$ v grupě. Je potřeba ukázat, že
libovolný $\boldsymbol{x} \in L$ je vektor $0 \cdot \boldsymbol{x}$ roven neutrálnímu prvku $\boldsymbol{o}$. K vektoru $0 \cdot \boldsymbol{x}$ ov

[jedinye] (A) Každá grupa má jen jediný neutrální/jednotkový prvek. Ke každému prvku grupy existuje jediný opačný/inverzní prvek.

Důkaz. (A) Předpokládáme dva neutrální prvky e_1, e_2. Musí platit $e_1 = e_1$ protože e_2 je neutrální. Musí také platit $e_2 = e_1 \circ e_2$, protože e_1 je neutr 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 n rální prvek. Pak platí: $y_1 = e \circ y_1 = (y_2 \circ x) \circ y_1 = y_2 \circ (x \circ y_1) = y_2 \circ e =$ takže $y_1 = y_2$.

[gruparesirovnice] Nechť na neprázdné množině G je dána operace $\circ :$ $G \to G$, pro kterou platí asociativní zákon (1) z definice grupy ??. Pak vlastn (2) a (3) z definice grupy jsou ekvivalentní s vlastností: pro každé a, b 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 ??. Ozna a^{-1} inverzní prvek k prvku a. Pak $x = a^{-1} \circ b$ řeší rovnici $a \circ x = b$, pro $a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b$. Z podobných důvodů $y = b \circ a^{-1}$ rovnici $y \circ a = b$.

Nechť nyní platí asociativní zákon (1) a umíme řešit uvedené rovn Volme $a \in G$. Označme e_a řešení rovnice $a \circ x = a$, tj. platí $a \circ e_a =$ Ukážeme nejprve, že pro libovolné $b \in G$ je $b \circ e_a = b$. Nechť $y \in G$ řeší rov $y \circ a = b$. Pak platí $b \circ e_a = (y \circ a) \circ e_a = y \circ (a \circ e_a) = y \circ a = b$. Vidíme t že řešení e_a rovnice $a \circ x = a$ nezávisí na volbě prvku a, takže stačí prve označovat e. Podobně lze ukázat, že také řešení rovnice $y \circ a = a$ nezávis volbě prvku a. Označme toto řešení f. Nyní podobně jako v důkazu věty $f \circ e = f$, protože e řeší $a \circ e = a$ a platí $f \circ e = e$, protože f řeší $f \circ a$ Takže $e = f$ a toto je jednotkový prvek grupy.

Sestrojíme inverzní prvek k prvku $x \in G$. Nechť u řeší rovnici $x \circ u =$ v řeší rovnici $v \circ x = e$. Platí $v = v \circ e = v \circ (x \circ u) = (v \circ x) \circ u = e \circ u$

Nechť G je grupa s operací $\circ$. Pokud $G_1 \subset G$ je sama o sobě gru
se stejnou operací (tj. speciálně $\circ \colon G_1 \times G_1 \to G_1$ a platí vlastnosti (1)
definice grupy ??), nazýváme G_1 *podgrupou* grupy G.

[podstruktura] Výše uvedenou definici uvádím hlavně proto, aby měl
nář možnost ji porovnat s definicí podprostoru ?? a shledal, že základní m
lenka definice podstruktury je pořád stejná. V případě ověřování podgrup
kontrola asociativního zákona (1) zbytečná (je zaručen už ve vnější grupě)
vlastnosti $x \circ y \in G_1$, $e \in G_1$ a existence inverzního prvku v G_1 jsou podsta

Množina $\mathbf{Z}$ celých čísel s operací sčítání „+“ je podgrupou grupy $\mathbf{R}$ r
ných čísel se stejnou operací.

Množina $\mathbf{Z} \setminus \{0\}$ celých nenulových čísel s operací násobení „·“ není p
grupou grupy $\mathbf{R} \setminus \{0\}$ reálných čísel se stejnou operací, protože k číslům růz
od -1 a 1 neexistuje na množině $\mathbf{Z} \setminus \{0\}$ inverzní prvek. Na druhé stran
jedná o pologrupu, protože násobení je uzavřeno na nenulová celá čísla
samozřejmě asociativní.

[dteleso] *Těleso* je množina T se dvěma operacemi obvykle označovan
$+ : T \times T \to T$ a $\cdot : T \times T \to T$, které mají následující vlastnosti:

(1) T s operací „+“ je komutativní grupa. Neutrální prvek této grup
označen symbolem 0.

(2) $T \setminus \{0\}$ s operací „·“ je komutativní grupa. Jednotkový prvek této gr
se značí symbolem 1.

(3) Operace „+“ a „·“ splňují distributivní zákon: $a \cdot (b + c) = a \cdot b + $

Někteří autoři v definici tělesa nepožadují komutativitu grupy vzhlede
násobení a pokud je splněna, mluví o *komutativním tělese*. Existují příkl
kdy komutativita násobení není splněna Důležitým příkladem jsou *kvaterni*
čísla podobná komplexním, ale se třemi nezávislými imaginárními jednotka
Kvaterniony se užívají například při popisu 3D transformací v počítačové
fice [28]. V našem textu budeme u těles vždy předpokládat komutativitu o
operací

prvek jako celé číslo. Toto je příklad struktury, která má všechny vlastnost lesa s výjimkou jediné: není zaručena existence inverzního prvku pro násob Taková struktura se nazývá *okruh*.

Množina komplexních čísel s operacemi sčítání a násobení tvoří těleso

[vteleso] Pro libovolné prvky a, b z tělesa platí: $a \cdot b = 0$ právě tehdy, k $a = 0$ nebo $b = 0$.

Důkaz. ($\Rightarrow$): $T \setminus \{0\}$ musí být podle vlastnosti (2) definice ?? vzhlede násobení grupa, tj. součin dvou nenulových prvků musí být prvek nenul Jinými slovy, pokud součin vychází nulový, musí aspoň jeden z činitelů nula.

($\Leftarrow$): Je třeba dokázat, že $0 \cdot a = 0$. Protože 0 je neutrální prvek vzhle ke sčítání, platí $0 + 0 = 0$. Díky distributivnímu zákonu je $0 \cdot a = (0 + 0) \cdot$ $0 \cdot a + 0 \cdot a$. K oběma stranám rovnosti přičteme opačný prvek k prvku 0 tedy prvek $-0 \cdot a$. Na levé straně dostáváme 0 a na pravé $0 \cdot a$.

[pZ2] Těleso musí podle definice obsahovat 0 a 1 a tyto dva prvky mu být různé. Takže těleso musí obsahovat aspoň dva prvky. Ukážeme, že exis těleso, které obsahuje jen tyto dva prvky, tedy $T = \{0, 1\}$.

Operaci „+" definujeme: $0 + 0 = 0,\ 0 + 1 = 1 + 0 = 1,\ 1 + 1 = 0$. Ope „·" definujeme jako obvyklé násobení: $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0,\ 1 \cdot 1 = 1$. Mno $T = \{0, 1\}$ s takto zavedenými operacemi tvoří těleso.

Skutečně, pro operaci „+" platí asociativní zákon, 0 je neutrální pr opačný prvek k 0 je 0 a opačný prvek k 1 je 1. Grupa $T \setminus \{0\}$ vzhlede násobení je jednoprvková a všechny vlastnosti grupy zde platí zcela samozře 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 *Galoi tělesa*. V našem příkladě $T = \{0, 1\}$ se tedy jedná o Galoisovo těleso se dv prvky.

Především 0 je neutrální prvek vzhledem ke sčítání, takže podle vlastnosti definice grupy ?? musí $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1$. Dále množina musí být grupou vzhledem k násobení, takže musí $1 \cdot 1 = 1$. Dále musí p $0 \cdot a = a \cdot 0 = 0$, jinak by nebyla splněna věta ??. Zbývá otázka, zda můž definovat $1 + 1 = 1$. Nemůžeme, protože pak by prvek 1 neměl prvek opač

[modulo] Na množině $\{0, 1, \ldots, p - 1\}$ definujme operace „+“ a „·“ obvyklé sčítání a násobení, ovšem na výsledek aplikujme proces „modulo Takže například pro $p = 5$ pracujeme s množinou $\{0, 1, 2, 3, 4\}$ a platí $4+3$ protože zbytek po dělení čísla 7 číslem 5 je 2. Nebo $4 \cdot 4 = 1$, protože zby po dělení čísla 16 číslem 5 je 1.

Nechť nejprve p není prvočíslo, tj. je tvaru součinu $p = m\,n$. Pak $m \cdot n$ modulo p, a přitom čísla m a n jsou nenulová. Podle věty ?? se nemůže jed o těleso, protože součin nenulových čísel musí v tělese vyjít jako číslo nenul

Nechť p je prvočíslo. Ukážeme, že $M = \{0, 1, \ldots, p - 1\}$ s operacemi $\cdot$ modulo p“ tvoří těleso. Především M se sčítáním modulo p je komutat grupa (viz příklad ??). Operace násobení modulo p je asociativní, komutat a jednotkovým prvkem je číslo 1. Distributivní zákon plyne z distributivn zákona běžných operací „+“ a „·“. Nejvíce práce dá nalezení inverzního pr pro $a \in M \setminus \{0\}$. Prvek a nechme pevný a uvažujme všechna čísla „ak mod p“ pro $k \in \{1, 2, \ldots, p - 1\}$. Tato čísla jsou pro různá k vzájemně různá níže) a pokrývají tedy celou množinu $\{1, 2, \ldots, p - 1\}$. Musí tedy exist takové k, že $ak = 1$ mod p. Toto k je inverzním prvkem k prvku a. V ú ještě chybí obhájit, že čísla „ak modulo p“ jsou pro různá k vzájemně rů Předpokládejme, že existují čísla $k_1, k_2 \in M \setminus \{0\}$, $k_1 \geq k_2$ taková, že ak ak_2 mod p, tj. $a(k_1 - k_2) = mp$ pro nějaké $m \geq 0$. Rovnost vydělíme čís a. Protože $a < p$ a p je prvočíslo, existuje $m_1 \geq 0$, že po vydělení čísle dostáváme $k_1 - k_2 = m_1 p$. Vlevo je číslo menší než p, takže musí být m_1 tj. $k_1 = k_2$.

Podle počtu prvků p se toto těleso označuje GF(p). Jiné značení **Z**

Charakteristika tělesa reálných čísel je ∞. Charakteristika tělesa $\mathbf{Z}_p$ j
[vcharakter] Charakteristika tělesa je nekonečná nebo to je prvočíslo.

Důkaz. Sporem. Nechť pro charakteristiku λ platí $\lambda = mn$, $m \neq \lambda$, $n \neq$
Z distributivního zákona plyne $(\sum_1^m 1) \cdot (\sum_1^n 1) = \sum_1^{mn} 1 = \sum_1^{\lambda} 1 = 0$. P
věty ?? musí být aspoň jedna suma v závorce rovna nule, protože jejich so
je nulový. To je spor s tím, že λ je nejmenší počet jedniček, jejichž souč
nulový.

Kromě GF(p), kde p je prvočíslo, existují konečná tělesa s počtem pr
p^m, kde p je prvočíslo, m je libovolná mocnina, značení: GF(p^m). Jak j
ukázali v příkladě ??, konstrukce operací pro GF(p^m) nemůže vycházet
z myšlenky „modulo p“. Ve skutečnosti je konstrukce tělesa GF(p^m) výra
komplikovanější. V následujícím příkladě je pro ilustraci popsáno těleso GF(

Z věty ?? plyne, že i tělesa GF(p^m) musejí mít charakteristiku ve tv
prvočísla. Kdybychom zde měli prostor na podrobnější popis těles GF(
shledali bychom, že mají charakteristiku p.

Dá se dále ukázat, že pokud má mít těleso konečný počet prvků, pak t
počet nemůže být jiný než p^m, kde p je prvočíslo a m přirozené číslo. N
operace na konečném tělese lze definovat jediným možným způsobem (liš
může jen způsob označení prvků).

[teleso6] Uvažujme množinu všech uspořádaných trojic prvků ze $\mathbf{Z}_2$ ind
vaných čísly. Nulová trojice nemá žádný index a ostatní trojice mají přiřaz
indexy 0 až 6:

$$\{(0,0,0)_*,\ (1,0,0)_0,\ (0,1,0)_1,\ (0,0,1)_2,\ (1,1,0)_3,\ (0,1,1)_4,\ (1,1,1)_5,\ (1,0$$

Prvky této množiny budeme sčítat tak, že si indexů nebudeme všímat a bud
sčítat jen uspořádané trojice v aritmetice $\mathbf{Z}_2$. Například $(1,1,0)_3 + (0,1,1$

Jak již bylo řečeno, je $(0,0,0)_*$ nulový prvek. Rovněž je zřejmé, že $(1,0$
je jednotkový prvek tohoto tělesa. Inverzní prvek například k $(0,0,1)_2$ je $(1,$
protože $2+5$ modulo $7=0$. Opačný prvek k libovolnému prvku x je prve
protože v aritmetice $\mathbf{Z}_2$ je $1+1=0$. Charakteristika tohoto tělesa je 2.

Prosím čtenáře, aby se nesnažil hrubou silou ověřit platnost distributiv
zákona tohoto tělesa (jde to, ale není to příliš účelné) ani příliš nehloubal
tím, proč například trojice $(1,1,1)$ má index 5. Pro odpovědi na tyto otázk
potřeba použít vlastnosti ireducibilních polynomů nad tělesem $\mathbf{Z}_2$ (obecně
tělesem $\mathbf{Z}_p$), což bohužel překračuje rámec tohoto úvodního textu.

V definici lineárního prostoru ?? jsme sice byli dostatečně abstraktní (
tory, ani operace s nimi jsme blíže nespecifikovali), ale pracovali jsme ta
docela konkrétní množinou $\mathbf{R}$ reálných čísel. Pokud v této definici nahrad
množinu $\mathbf{R}$ pojmem těleso (s blíže nespecifikovanými prvky a operacemi),
stáváme lineární prostor nad tělesem. Můžeme pak pracovat s lineárním
storem nad tělesem komplexních čísel, lineárním prostorem nad tělesem
atd.

Pokusíme se tedy do třetice přepsat definici lineárního prostoru, tento
nad libovolným tělesem.

[dlpT] Množinu L nazýváme *lineárním prostorem nad tělesem T*, po
jsou definovány operace $+: L\times L \to L$ a $\cdot: T\times L\to L$ tak, že L tvoří s ope
$+$ komutativní grupu, a dále $\forall \alpha,\beta\in T, \forall \boldsymbol{x},\boldsymbol{y}\in L$:

$$
\begin{aligned}
&\text{(A)} \quad \alpha\cdot(\beta\cdot\boldsymbol{x}) = (\alpha\cdot\beta)\cdot\boldsymbol{x},\\
&\text{(B)} \quad \alpha\cdot(\boldsymbol{x}+\boldsymbol{y}) = \alpha\cdot\boldsymbol{x}+\alpha\cdot\boldsymbol{y},\\
&\text{(C)} \quad (\alpha+\beta)\cdot\boldsymbol{x} = \alpha\cdot\boldsymbol{x}+\beta\cdot\boldsymbol{x},\\
&\text{(D)} \quad 1\cdot\boldsymbol{x} = \boldsymbol{x}.
\end{aligned}
$$

Volíme-li za těleso T v této definici množinu reálných čísel $\mathbf{R}$, dostáv

[LPTn] Vrátíme se k příkladu lineárního prostoru reálných uspořádan n-tic ?? a zobecníme ho na lineární prostor uspořádaných n-tic prvků libo ného tělesa.

Nechť T je těleso. Uvažujme množinu uspořádaných n-tic prvků z těles (označme ji T^n) a definujme na ni operace $+ : T^n \times T^n \to T^n$, $\cdot : T \times T^n \to$ 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 l ární prostor nad tělesem T.

Volíme-li za těleso $T = \mathbf{Z}_2$, je T^n podle předchozího příkladu diskrétn neární prostor, který je používán v teorii kódování. Jednotlivé vektory (tzv nární slova) jsou uspořádané n-tice jedniček a nul. Tento lineární prostor celkem 2^n různých vektorů.

V případě lineárního prostoru nad konečným tělesem dostáváme kone lineární prostor. V tomto případě tedy neplatí tvrzení poznámky ??. Mů si všimnout, že toto tvrzení se opíralo o skutečnost, že „reálných čísel je konečně mnoho“. Poznámka ?? zůstává v platnosti pro lineární prostory nekonečnými tělesy.

16. Lineární algebra v teorii kódování

Teorie kódování řeší otázku, jak převést danou informaci do slov, k
používají znaky nějaké abecedy (obvykle abecedy jedniček a nul) pokud mo
efektivně, tj. bez zbytečného zatěžování přenosových linek a paměťových m
nadbytečnými informacemi. Typickým příkladem kódování je ASCII kód, k
písmenům anglické abecedy a běžným znakům přiřazuje sedmibitová sl
Navíc se při kódování často řeší otázka, jakým způsobem efektivně přid
zakódované informaci dodatečné bity tak, aby byla informace odolná vůči š
na přenosové lince nebo menším chybám na paměťovém médiu. Dekodér
zařízení, které má za úkol restaurovat původní informaci, může být postave
nekvalitní linkou a může tedy dostat informaci zkreslenou. Z vhodně navržen
dodatečných bitů může dekodér zjistit, zda informace při průchodu linkou
poškozena a v lepším případě dokáže chybu také opravit.

Při návrhu vhodného kódování s možností detekce a opravy chyb s
od padesátých let minulého století používala lineární algebra. Tuto kapi
završíme příkladem konstrukce tzv. lineárních Hammingových kódů. To sa
zřejmě zdaleka nepokrývá veškerou problematiku teorie kódování, zájem
další studium této problematiky může použít třeba [1].

Někteří laici možná nerozlišují slovo kódování od slova šifrování. Šifro
je převod informace do takového stavu, aby ji bylo možné zpětně zrestaur
jen pověřenými osobami. Tuto problematiku, ačkoli matematicky rovněž v
zajímavou a ze strategického hlediska velmi důležitou, zde řešit nebudeme

Definice lineárního prostoru ?? předpokládá, že skaláry (čísla, kterými
sobíme vektory) jsou reálná čísla. V této kapitole budeme pracovat s modi
vanou definicí lineárního prostoru, kde reálná čísla nahradíme tělesem $\mathbf{Z}_2$.

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

·	0	1
0	0	0
1	0	1

Tedy: $0+0=0, \quad 0+1=1+0=1, \quad 1+1=0, \quad 0\cdot 0 = 0\cdot 1 = 1 \cdot 0$ $1 \cdot 1 = 1.$

Sčítání na $\mathbf{Z}_2$ je shodné s logickou operací XOR (vylučovací nebo) a n bení 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 č 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 s číslo a prvek 1 jako jakékoli číslo liché. Sčítáme a násobíme pak sudá čísl sudými, s lichými atd. Tyto operace pak dávají jako výsledek čísla sudá n lichá přesně podle pravidel počítání v $\mathbf{Z}_2$.

Nebo ještě jinak: provedeme operaci sčítání a násobení jako v příp celých čísel, ale pokud výsledek padne mimo množinu $\{0,1\}$, použijeme zby při dělení výsledku číslem 2.

Na množině uspořádaných n-tic prvků ze $\mathbf{Z}_2$, tj. na množině $\mathbf{Z}_2^n$, z deme operaci sčítání $+ \colon \mathbf{Z}_2^n \times \mathbf{Z}_2^n \to \mathbf{Z}_2^n$ analogicky, jako v případě sčí uspořádaných n-tic reálných čísel, jen samozřejmě pracujeme se sčítáním p definice ??. Pro $(a_1,\ldots,a_n) \in \mathbf{Z}_2^n$ a $(b_1,\ldots,b_n) \in \mathbf{Z}_2^n$ definujeme

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

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 n přirozeným způsobem:

„nad tělesem“ (podrobněji viz definici ??). V tomto příkladě jsme zavedl
množině $\mathbf{Z}_2^n$ operace tak, že dostáváme *lineární prostor nad tělesem $\mathbf{Z}_2$*.

Nulový vektor tohoto lineárního prostoru je vektor $(0, \ldots, 0)$. Tento l
ární prostor má celkem 2^n vektorů, které mezi sebou umíme sčítat a samozře
tyto vektory umíme násobit jedničkou nebo nulou.

Na rozdíl od lineárních prostorů nad $\mathbf{R}$ náš nově zavedený lineární pro
nad $\mathbf{Z}_2$ má konečně mnoho prvků. To je jediný rozdíl vzhledem k lineár
prostorům, které jsme dosud studovali. Všechny ostatní vlastnosti zůstá
stejné.

Každý vektor z $\mathbf{Z}_2^n$ je sám sobě opačným vektorem, tj. $\forall \boldsymbol{x} \in \mathbf{Z}_2^n : \boldsymbol{x} =$
neboli $\boldsymbol{x} + \boldsymbol{x} = \boldsymbol{o}$. Díky tomu v tělese $\mathbf{Z}_2$ a v lineárním prostoru nad tí
tělesem nemusíme rozlišovat mezi sčítáním a odčítáním.

[Z2M] 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
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
tři.

Protože $\mathbf{Z}_2^n$ obsahuje konečný počet vektorů, můžeme (na rozdíl od lin
ních prostorů nad $\mathbf{R}$) vypsat podprostor nebo lineární obal výčtem prvků.
podprostor M z předchozího příkladu platí:

lineární kombinace, které můžeme s vektorem $\boldsymbol{x}$ vytvořit. Množina M má prvkovou bázi $\{\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}\}$. Takže pro sestavení lineárního obalu stačí najít všec lineární kombinace těchto tří vektorů: $\boldsymbol{o}$, $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, $\boldsymbol{a}+\boldsymbol{b}$, $\boldsymbol{a}+\boldsymbol{c}$, $\boldsymbol{b}+\boldsymbol{c}$, $\boldsymbol{a}+\boldsymbol{b}$

Zjistěte počet prvků lineárního (pod)prostoru nad $\mathbf{Z}_2$, který má dimen

Řešení: Má-li (pod)prostor dimenzi n, pak má n prvkovou bázi $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots$ Abychom získali všechny lineární kombinace těchto vektorů, musíme každý tor násobit jedničkou nebo nulou. Máme tedy 2^n lineárních kombinací. T kombinace vyplňují celý lineární (pod)prostor a jsou navzájem různé. Kd se totiž dvě lineární kombinace s různými koeficienty rovnaly, pak jejich čtením dostáváme netriviální lineární kombinaci rovnu nulovému vektoru 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. příklad podprostor M z příkladu ?? má dimenzi 3 a má tedy $2^3 = 8$ prvků

Najděte všechna řešení $\boldsymbol{x} \in \mathbf{Z}_2^6$ homogenní soustavy rovnic $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$, j

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

Řešení: Najdeme matici ekvivalentní soustavy s lineárně nezávislými ř

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Hodnost matice soustavy je 4, dimenze prostoru je 6, takže dimenze n

Při hledání báze prostoru řešení můžeme také využít větu ??. V předcho
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 t
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 $-\mathbf{C}$, proto
aritmetice $\mathbf{Z}_2$ jsou obě matice stejné.

[dkod] Nechť A je konečná množina (tzv. *abeceda*). Pak *slovo* je libov
konečná posloupnost prvků z A.

Kódování v obecném smyslu zahrnuje (1) algoritmus, kterým inforn
převádíme do posloupnosti slov (tzv. *kodér*) a (2) algoritmus, kterým zp
z těchto slov získáváme původní informaci (*dekodér*).

Slova, která vytváří kodér, se nazývají *kódová slova*. Množina všech k
vých slov se nazývá *kód*.

Je-li kód množinou slov stejné délky (každé kódové slovo má stejný p
znaků abecedy), mluvíme o tzv. *blokovém kódu*. Blokový kód *délky n* znač
všechna kódová slova mají n znaků abecedy.

Typicky $A = \{0, 1\}$, tj. abeceda se skládá jen ze dvou znaků (tzv. b
anglicky bits, což je původně zkratka z BInary digiTS) a slova jsou posloupn
těchto bitů.

ASCII kód je množina 7bitových slov, která reprezentují jednotlivá
mena anglické abecedy a další běžné znaky (číslice, tečku, vykřičník, otaz

prezentován jako množina 8bitových slov. Později začal být tento bit využi pro různá rozšíření ASCII kódu, která zahrnují i reprezentaci některých písi s diakritickými znaménky.

Je potřeba si uvědomit, že slova jsou do paměťového média nebo do nosové linky vkládána za sebou bez oddělovačů. Blokový kód má tu výhodu dekodér dokáže snadno rozdělit tento „tok znaků abecedy“ na slova a těm přidělit význam například pomocí nějaké tabulky. Nevýhoda blokového k spočívá v tom, že plýtvá místem, neboť tušíme, že pokud navrhneme pro ča se vyskytující slova kratší posloupnosti znaků, celkový počet znaků abecedy přenášené/ukládané informace může být menší. To ostatně je (alespoň zhru i vlastnost přirozeného jazyka. Tam máme ovšem abecedu rozsáhlejší (n nární) a za prvek abecedy můžeme považovat i mezeru: oddělovač mezi sl který dekodéru pomůže. Nebo v Morseově abecedě máme také tři znaky: te čárka a mezera. Bez mezery by bylo dekódování morseovky nemožné. Mán k dispozici jen binární abecedu $A = \{0, 1\}$, pak je potřeba při návrhu k se slovy nestejné délky myslet na možnosti dekodéru. Je to technicky mo ale není to obsahem tohoto textu. Příkladem neblokového kódu je UTF8, k kóduje znaky abeced všech jazyků světa. Písmena anglické abecedy a b znaky jsou reprezentovány 8bitovým slovem, ale písmena dalších jazyků kódována 16bitovým slovem nebo i delším (24 bitů a 32 bitů).

Nadále budeme pracovat jen s blokovými kódy nad binární abecedou.

Nechť K je blokový kód délky n nad binární abecedou A. Pak platí A A^n.

Pokud $K \neq A^n$, pak mezi uspořádanými n-ticemi z A existují nekód slova, tj. taková, která kodér nikdy nevytvoří a která nemají přidělen význ Přijme-li dekodér (např. za nekvalitní linkou) nekódové slovo, je si jist, že přenosu linkou došlo k chybě. Může například v takovém případě požádat mocí jiných technických prostředků kodér, aby vyslal slovo znovu. Neb může pokusit chybu opravit.

velmi často schopni detekovat i opravit. Někdy ale překlep může způsobit vzniká jiné běžné slovo jazyka. Člověk jako dekodér ani s tímto druhem ch nemá většinou problém, protože pracuje s kontextem celé věty (větší sku slov). Takto inteligentní dekodér ale nebude naším cílem. Vystačíme si s d kováním a opravováním chyb jen na úrovni jednotlivých slov.

[hammingd] Nechť $A = \{0, 1\}$. *Hammingova velikost slova* $\boldsymbol{u} \in A^n$ je p jedniček v tomto slově a značíme ji $\|\boldsymbol{u}\|$. *Hammingova vzdálenost slov* $\boldsymbol{v} \in$ *a* $\boldsymbol{w} \in A^n$ je počet bitů, ve kterých se tato dvě slova liší. Značíme ji $\mathrm{d}(\boldsymbol{v}, \boldsymbol{w}$

[hammingp] Nechť $A = \{0, 1\}$ a $\boldsymbol{v}, \boldsymbol{w} \in A^n$. Pak $\boldsymbol{v} + \boldsymbol{w}$ (v aritmetice je slovo, které má jedničky právě v místech, kde se $\boldsymbol{v}$ a $\boldsymbol{w}$ liší. Takže p $\mathrm{d}(\boldsymbol{v}, \boldsymbol{w}) = \|\boldsymbol{v} + \boldsymbol{w}\|$.

Předpokládejme, že $\boldsymbol{v}$ je slovo vyslané kodérem a $\boldsymbol{w}$ slovo přijaté dek rem. Pak $\mathrm{d}(\boldsymbol{v}, \boldsymbol{w})$ udává počet chyb ve slově, které vznikly během přenosu

Poznámka v poznámce: předpokládáme, že díky technickým paramet zařízení nikdy nedojde k chybě, kdy se jednička nebo nula ze slova zcela vyt nebo vznikne nová, tj. nikdy nehrozí riziko, že by na straně dekodéru byl pře jiný počet jedniček a nul než byl vyslán kodérem.

[kod2] Je dán tento kód: $K = \{0000, 0011, 0101, 1001, 0110, 1010, 1100,$ Jedná se o blokový binární kód délky 4. Pro potřeby tohoto příkladu nebud specifikovat druh informace, kterou potřebujeme přenášet. Protože kód o huje jen 8 slov, může být původní informace zapsána pomocí nějaké 8 znak abecedy.

Zajímavé na tomto kódu je, že každé kódové slovo obsahuje sudý počet niček. Pokud dojde k jediné chybě ve slovu, máme jistotu, že dekodér př nekódové slovo (s lichým počtem jedniček) a ohlásí chybu. Je-li pravděpo nost výskytu dvou nebo více chyb v jednom slově zanedbatelná a nám posta jen detekovat chyby (neopravovat je), je toto rozumný návrh kódu.

Povšimneme si, že minimální Hammingova vzdálenost mezi dvěma tého slova $\boldsymbol{w}$ vrátí ke kódovému slovu $\boldsymbol{v}$ takovému, že Hammingova vzdále $\mathrm{d}(\boldsymbol{v}, \boldsymbol{w}) = 1$. Samozřejmě, naučíme-li dekodér opravovat jednu chybu ve sl pak už nemusí být schopen vždy správně detekovat tři chyby. Může se t stát, že místo toho opraví jeden bit a dostane jiné kódové slovo.

[vzdalenost+oprava] Nechť minimální Hammingova vzdálenost mezi dovými slovy je $d > 2$. Rozhodněte (A) kolik chyb ve slově může deke detekovat, pokud po něm nechceme, aby chyby opravoval, a (B) kolik chy slově může opravit a kolik jich může aspoň detekovat bez opravy.

Odpověď: (A) Dekodér může spolehlivě detekovat nejvýše $d - 1$ chyb. Je-li d sudé, může dekodér opravit jednu až $d/2 - 1$ chyb a detekovat $d/2$ c bez opravy. Je-li d liché, může opravit jednu až $(d-1)/2$ chyb a žádné množ chyb nedetekuje bez opravy. Je samozřejmě možné i jiné rozvržení. Např. d liché necháme dekodér opravit nejvýše $(d-3)/2$ chyb a při výskytu $(d-$ nebo $(d+1)/2$ chyb ve slově jen chyby detekujeme bez opravy.

Při návrhu dekodéru s detekcí nebo opravou chyb se s výhodou vy nástroje lineární algebry, jako je násobení matic, vymezení podprostorů a b řešení homogenních soustav atd. Binární slova délky n budeme v tomto příp považovat za vektory z lineárního prostoru $\mathbf{Z}_2^n$, takže je můžeme sčítat. Osta už v poznámce ?? jsem zmínil sčítání slov $\boldsymbol{v}$ a $\boldsymbol{w}$. V teorii kódování se bin slova zapisují jedničkami a nulami bez mezer (viz příklady ?? a ??), zatí v lineární algebře jsme dosud zapisovali vektory do závorek a jejich slo oddělovali čárkami. Věřím, že nedojde k nedorozumění, pokud dále v tex kódování budu zapisovat vektory způsobem, jako v příkladu ??.

[dlkod] Binární blokový kód K délky n je *lineární*, pokud K tvoří l ární podprostor lineárního prostoru $\mathbf{Z}_2^n$. Jestliže dimenzi tohoto podpros označíme k, pak mluvíme o *lineárním (n, k) kódu*.

[nejmhm] Nejmenší Hammingova vzdálenost mezi slovy lineárního kód je rovna nejmenší Hammingově velikosti nenulového kódového slova.

Báze kódu z příkladu ?? je například $\{0011, 0101, 1100\}$, takže dime kódu je 3 a jedná se tedy o *lineární* $(4,3)$ *kód*.

Příklad ?? ilustruje tzv. kódování s kontrolním bitem parity. Původní in maci s osmi znaky je možné kódovat blokovým binárním kódem $\{000, 001, 01$ tedy stačí nám tři bity. Pokud chceme detekovat jednu chybu ve slově, přid čtvrtý tzv. *kontrolní bit*, který nastavíme na 0, pokud je v původním tříbito slově sudý počet jedniček a nastavíme ho na 1, pokud je v původním slově l počet jedniček. Dostáváme tak kód z příkladu ??.

Tento postup můžeme použít na jakýkoli „výchozí“ binární blokový délky k se všemi 2^k kódovými slovy. Přidáním kontrolního bitu parity do váme lineární $(k+1, k)$ kód, kterým jsme schopni detekovat jednu chybu slově. Dekodér pak odstraní kontrolní bit z každého přijatého slova a získá původní kódovanou informaci.

Vstupní informace je často připravena už jako posloupnost slov binár blokového kódu délky k, ve kterém všechna slova jsou kódová. Naším úko je pak rozšířit tento kód o dalších $n-k$ tzv. *kontrolních bitů*, abychom do lineární (n,k) kód. Kodér tedy očekává na vstupu libovolné slovo délky jeho úkolem je zkopírovat bity vstupu do výstupu (tzv. *informační bit* přidat $n-k$ kontrolních bitů. Dekodér pak použije tyto kontrolní bity detekci a případnou opravu chyb a poté je odstraní a ponechá jen inform bity. Cílem je navrhnout kódování, které má co nejmenší *redundanci* (tj. po počtu kontrolních bitů ku počtu všech přenášených bitů ve slově), protož zatěžuje linku nebo paměťové médium režijními informacemi, které uživate svého pohledu nevyužije. Přitom ale chceme co nejschopnější dekodér, kter detekoval a opravoval chyby a navíc by měl pracovat efektivně.

Z pohledu lineární algebry je výše popsaný přechod od kódu délky k lineární kód délky $n > k$ lineární zobrazení $\mathcal{A}\colon \mathbf{Z}_2^k \to \mathbf{Z}_2^n$, které je prosté (j by docházelo ke ztrátě informace). Podle poznámky ?? množina obrazů tol zobrazení (neboli kód) tvoří lineární podprostor v $\mathbf{Z}_2^n$. Bázi tohoto pod neumí.

[doublekod] Nechť je vstupní informace kódována binárním blokovým
dem délky k se všemi 2^k slovy. Kodér této informace navrhneme tak, že ka
vstupní slovo zopakuje a vytvoří výstupní slovo délky $2k$. Tím vzniká line
$(2k, k)$ kód. Minimální Hammingova vzdálenost mezi dvěma kódovými s
je 2, takže dekodér spolehlivě detekuje jednu chybu ve slově. Za jistých o
ností může detekovat i více chyb ve slově, pokud chyba v první polovině s
se nezopakuje na stejném bitu druhé poloviny slova. V žádném případě
dekodér nemůže odhalenou chybu spolehlivě opravit. Redundance je příliš
soká, a přitom neumíme ani opravit chyby. Asi to nebude nejlepší možný na
kódování.

Kód z příkladu ?? je lineární. Nevýhoda tohoto kódu ale spočívá v t
že kódová slova mohou reprezentovat jen čtyři rozdílné stavy původní in
mace, ale mají příliš mnoho bitů, které zbytečně zatěžují paměťové méd
nebo přenosové linky. Proto se Hamming zaměřil na hledání jiných vhod
ších lineárních kódů.

[dHG] *Generující matice lineárního kódu K* je po řádcích zapsaná
tohoto kódu.

Kontrolní matice lineárního kódu K je taková matice $\mathbf{H}$ s lineárně n
vislými řádky, pro kterou platí: množina řešení homogenní soustavy $\mathbf{H}\,\boldsymbol{x}$
je rovna kódu K.

[vlHG] Nechť $\mathbf{G}$ je generující matice a $\mathbf{H}$ kontrolní matice lineárního (
kódu. Pak $\mathbf{G}$ má k řádků a $\mathbf{H}$ má $n - k$ řádků. Obě matice mají n slou
Jinými slovy, generující matice má tolik řádků, kolik je v kódu informač
bitů, kontrolní matice má tolik řádků, kolik má kód kontrolních bitů a p
sloupců obou matic je roven počtu přenášených bitů v jednom slově.

Důkaz. Matice $\mathbf{G}$ má k řádků, protože báze prostoru dimenze k obsahu
vektorů. Počet řádků matice H plyne z věty ?? Konečně n sloupců obou m

protože $\{1001, 0101, 0011\}$ je báze kódu K. Popíšu, jak se obvykle tato b
sestavuje. Vyjde se ze standardní báze vstupního kódu: $\{100, 010, 001\}$ a a
kuje se na ní zobrazení kodéru. Všechny tři prvky této báze mají lichý p
jedniček, takže poslední kontrolní bit kodér nastaví na jedničku.

Kontrolní matice našeho kódu je

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix},$$

protože množina řešení rovnice $x_1+x_2+x_3+x_4 = 0$ je shodná s množinou s
které mají sudý počet jedniček (sčítáme jedničky modulo 2), a to jsou p
všechna kódová slova.

[doublekod2] Kódujme vstupní informaci v blokovém kódu délky 4 p
příkladu ?? (zdvojení slova). Dostáváme lineární (8,4) kód. Jeho generující
tice 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 příkl
Na standardní bázi prostoru $\mathbf{Z}_2^4$ jsem aplikoval zobrazení kodéru. Kontr
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, dr
šestému, třetí sedmému a čtvrtý osmému, tj. obě části slova se rovnají a je

Důkaz. Kód s uvedenými maticemi označíme písmenem K. Řádky matic
alias sloupce matice $\mathbf{G}^T$ jsou podle definice generující matice prvky kódu
Podle definice kontrolní matice musí tyto sloupce matice $\mathbf{G}^T$ alias prvky k
K být řešením soustavy $\mathbf{H}\,\boldsymbol{x} = \boldsymbol{o}$. Přesně to říká vztah $\mathbf{H} \cdot \mathbf{G}^T = \mathbf{O}_1$, po
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 st
vztahu $\mathbf{H} \cdot \mathbf{G}^T = \mathbf{O}_1$.

[odGkH] Předchozí věta ukazuje, že nejen řádky matice $\mathbf{G}$ řeší soust
$\mathbf{H}\boldsymbol{x} = \boldsymbol{o}$, ale také řádky matice $\mathbf{H}$ řeší soustavu $\mathbf{G}\boldsymbol{x} = \boldsymbol{o}$. Známe-li jen jed
těchto matic, pak druhou lze najít tak, že najdeme bázi množiny řešení od
vídající homogenní soustavy rovnic a zapíšeme ji do řádků.

Protože velmi často je generující matice vytvořena za použití standa
báze vstupního prostoru $\mathbf{Z}_2^k$ a aplikací algoritmu kodéru na tuto bázi, k
kopíruje informační bity a přidává kontrolní bity na konec slova, je matic
často ve tvaru $\mathbf{G} = (\mathbf{E}|\mathbf{C})$, kde $\mathbf{E}$ je jednotková matice typu (k, k). Matic
pak můžeme snadno najít podle věty ??, přitom místo matice $-\mathbf{C}^T$ stačí po
matici $\mathbf{C}^T$, protože v aritmetice $\mathbf{Z}_2$ je $\mathbf{C} = -\mathbf{C}$. Dostáváme $\mathbf{H} = (\mathbf{C}^T|\mathbf{E}')$,
$\mathbf{E}'$ je jednotková matice typu $(n-k, n-k)$.

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.
je tedy řádek jedniček, ke kterému podle věty ?? vpravo připíšeme jednotko
matici typu $(1, 1)$. Dostáváme matici $\mathbf{H}$.

Příklad ??. Matice $\mathbf{C}$ z rovnosti $\mathbf{G} = (\mathbf{E}|\mathbf{C})$ je jednotková matice, t
$\mathbf{C}^T = \mathbf{C}$. K této jednotkové matici podle věty ?? připíšeme jednotkovou m
typu $(4, 4)$. Dostáváme tím matici $\mathbf{H}$, která je výjimečně rovna matici $\mathbf{G}$.

[dsystemkod] Pokud existuje generující matice lineárního kódu ve t
$\mathbf{G} = (\mathbf{E}|\mathbf{C})$, kde $\mathbf{E}$ je jednotková matice, nazýváme takový kód *systematic*

[HGprechod] Předchozí poznámka ?? ukazuje, že pro systematické k nemění lineární obal řádků. Může se tedy stát, že po eliminaci dostaneme no 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 ($\mathbf{E}$ jedná se o nesystematický kód. I v tomto případě je ovšem eliminací možné spět k matici, která se od matice $(\mathbf{E}|\mathbf{C})$ liší jen prohozením některých slou Nesystematický kód se tedy od systematického liší jen pořadím bitů v notlivých kódových slovech. Přechod od generující matice ke kontrolní (n obráceně) je u nesystematického kódu obtížnější, protože nelze přímo po větu ??, ale před jejím použitím musíme prohodit sloupce generující ma pak přejít ke kontrolní matici a u ní prohodit sloupce zpět. Podobně bych postupovali, pokud přecházíme od kontrolní matice nesystematického kód matici generující.

Systematický kód získáme zaručeně v případě, kdy necháme kodér k rovat informační bity vstupního slova do výstupu a pak přidat bity kontr Pokud ale kodér informační bity „promíchá" s bity kontrolními, pak kód ne být systematický.

[HDE] Kód je systematický právě tehdy, když existuje kontrolní ma tohoto kódu tvaru $(\mathbf{C}^T|\mathbf{E}')$, kde $\mathbf{E}'$ je jednotková matice.

Důkaz. Tvrzení věty je důsledkem skutečnosti, že kód má generující ma tvaru $\mathbf{G} = (\mathbf{E}|\mathbf{C})$ právě tehdy, když má kontrolní matici tvaru $\mathbf{H} = (\mathbf{C}^T|\mathbf{E}$

[elimH] Je-li dána kontrolní matice v jiném tvaru než $(\mathbf{C}^T|\mathbf{E}')$, pak z t ještě neplyne, že kód není systematický. Eliminací kontrolní matice můž získat jinou kontrolní matici, která ovšem přísluší stejnému kódu. Stačí si v domit, že eliminací matice soustavy dostáváme případně matici jiné soust ale se stejnou množinou řešení. Pokud tedy po eliminaci kontrolní matice káme matici tvaru $(\mathbf{C}^T|\mathbf{E}')$, pak je kód systematický.

[koderzob] Nechť $\mathbf{G}$ je generující matice lineárního (n,k) kódu. Nechť $A: \mathbf{Z}_2^k \to \mathbf{Z}_2^n$ je lineární zobrazení, které zobrazuje standardní bázi prostoru obrazů (při zobrazení $\mathcal{A}$) standardní báze $\mathbf{Z}_2^k$ vzhledem ke standardní bá $\mathbf{Z}_2^n$. Abychom z řádků matice dostali sloupce podle definice matice lineár zobrazení, stačí matici $\mathbf{G}$ transponovat.

Zobrazení $\mathcal{A}$ z předchozí věty matematicky popisuje kodér lineárního k Jeho generující matice je $\mathbf{G}$. Věta říká, že $\mathbf{G}^T$ je matice zobrazení tohoto ko vzhledem ke standardním bázím. Vstupuje-li vektor $\boldsymbol{u} \in \mathbf{Z}_2^k$ do kodéru, pak výstupem je vektor $\boldsymbol{v} \in \mathbf{Z}_2^n$, který spočítáme podle věty ?? jako součin ma zobrazení a vstupního vektoru:

$$\boldsymbol{v}^T = \mathbf{G}^T \cdot \boldsymbol{u}^T, \qquad \text{neboli:} \quad \boldsymbol{v} = \boldsymbol{u} \cdot \mathbf{G}.$$

[jenkontrolni] Pokud kodér kopíruje k vstupních bitů do výstupu a přidá kontrolní bity, nemusíme prvních k bitů výstupu počítat maticovým sobením. Stačí tímto násobením počítat kontrolní bity. Generující matice n tomto případě tvar $\mathbf{G} = (\mathbf{E}|\mathbf{C})$. Označíme-li $\boldsymbol{u}$ slovo, které vstupuje do ko a $\boldsymbol{v}'$ vektor, který obsahuje jen kontrolní bity výstupního slova, pak platí:

$$\boldsymbol{v}' = \boldsymbol{u} \cdot \mathbf{C}.$$

Dekodér při kontrole, zda se jedná o kódové slovo, použije kontrolní ma Nechť dekodér přijme slovo $\boldsymbol{w}$. Pak $\mathbf{H} \cdot \boldsymbol{w}^T$ je nulový vektor právě tehdy, k je slovo $\boldsymbol{w}$ kódové. V takovém případě dekodér předpokládá, že nedošlo přenosu slova k chybě, odstraní kontrolní bity a tím získá původní informa

Pokud $\mathbf{H} \cdot \boldsymbol{w}^T$ není nulový vektor, dekodér má jistotu, že došlo k chy že $\boldsymbol{w}$ není kódové slovo. Má-li chybu opravit, pak údaj $\mathbf{H} \cdot \boldsymbol{w}^T$ bude při op potřebovat. Napíšeme-li výsledek násobení $\mathbf{H} \cdot \boldsymbol{w}^T$ do řádku, dostáváme *syndrom* vektoru $\boldsymbol{w}$.

[dsyndrom] Nechť $\mathbf{H}$ je kontrolní matice lineárního kódu. *Syndrom* s $\boldsymbol{w}$ je vektor $\boldsymbol{s}$, pro který platí $\boldsymbol{s}^T = \mathbf{H} \cdot \boldsymbol{w}^T$

Než se pustíme do sestavování tabulky, podle které bude dekodér oprav chyby, je potřeba si uvědomit platnost dvou tvrzení. První z nich platí dok obecně na libovolném lineárním prostoru.

[afinM1M2] Nechť K je lineární podprostor lineárního prostoru L a n $\boldsymbol{e}_1 \in L$, $\boldsymbol{e}_2 \in L$. Pak množiny $M_1 = \{\boldsymbol{e}_1 + \boldsymbol{v};\ \boldsymbol{v} \in K\}$, $M_2 = \{\boldsymbol{e}_2 + \boldsymbol{v};\ \boldsymbol{v} \in$ jsou buď disjunktní nebo totožné.

Důkaz. Sporem. Předpokládáme, že množiny M_1 a M_2 mají společný bod přitom nejsou totožné, tj. existuje vektor $\boldsymbol{b} \in M_1$, který neleží v M_2. Pro $\boldsymbol{a}$ 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. $\boldsymbol{w} = \boldsymbol{b} - \boldsymbol{a} = \boldsymbol{v} - \boldsymbol{u}$ leží v K, protože K je podprostor. Je tedy $\boldsymbol{b} = \boldsymbol{a}$ - Protože $\boldsymbol{a}$ leží i v množině M_2, je $\boldsymbol{a} = \boldsymbol{e}_2 + \boldsymbol{x}$, kde $\boldsymbol{x} \in K$. Dosadíme-li t poznatek do vztahu pro $\boldsymbol{b}$, dostaneme $\boldsymbol{b} = \boldsymbol{e}_2 + \boldsymbol{x} + \boldsymbol{w}$. Protože K je podpros $\boldsymbol{x} + \boldsymbol{w}$ leží v K. Je tedy $\boldsymbol{b} = \boldsymbol{e}_2 + \boldsymbol{z}$, kde $\boldsymbol{z} \in K$. To ale znamená, že $\boldsymbol{b} \in$ což je sporu s předpokladem.

[osyndromu] Nechť $\boldsymbol{v}$ je kódové slovo a $\boldsymbol{e}$ je libovolné slovo. Pak slo i $\boldsymbol{e} + \boldsymbol{v}$ mají stejný syndrom. Jinými slovy kódová slova modifikovaná ste chybou vytvářejí skupinu slov se společným syndromem.

Důkaz. $\mathbf{H} \cdot (\boldsymbol{e} + \boldsymbol{v})^T = \mathbf{H} \cdot \boldsymbol{e}^T + \mathbf{H} \cdot \boldsymbol{v}^T = \mathbf{H} \cdot \boldsymbol{e}^T + \boldsymbol{o}^T = \mathbf{H} \cdot \boldsymbol{e}^T$.

Pokud požadujeme nejen detekci, ale i opravu chyb lineárního kódu, n dekodér pracovat s následující *tabulkou pro opravování chyb*:

$\boldsymbol{o}$	$\boldsymbol{o}$	$\boldsymbol{v}_2$	$\boldsymbol{v}_3$	$\dots$	$\boldsymbol{v}$
$\boldsymbol{s}_2$	$\boldsymbol{e}_2$	$\boldsymbol{e}_2 + \boldsymbol{v}_2$	$\boldsymbol{e}_2 + \boldsymbol{v}_3$	$\dots$	$\boldsymbol{e}_2 +$
$\boldsymbol{s}_3$	$\boldsymbol{e}_3$	$\boldsymbol{e}_3 + \boldsymbol{v}_2$	$\boldsymbol{e}_3 + \boldsymbol{v}_3$	$\dots$	$\boldsymbol{e}_3 +$
$\dots$	$\dots$				
$\boldsymbol{s}_{2^{(n-k)}}$	$\boldsymbol{e}_{2^{(n-k)}}$	$\boldsymbol{e}_{2^{(n-k)}} + \boldsymbol{v}_1$	$\boldsymbol{e}_{2^{(n-k)}} + \boldsymbol{v}_2$	$\dots$	$\boldsymbol{e}_{2^{(n-k)}}$

slova, která chceme, aby dekodér uměl odhalit a chybu opravit. Na ostat pozicích tabulky jsou součty chybového slova v řádku s kódovým sloven sloupci.

Tabulku vytvoříme tak, že zapíšeme nejprve do prvního řádku nulové dové slovo a pak ostatní kódová slova (na pořadí nezáleží). Do druhého řá napíšeme nejprve chybové slovo, které chceme dekodérem opravovat, a příslušné součty. Chybové slovo nesmí být slovem kódovým. Na třetím řá napíšeme další chybové slovo. Toto chybové slovo se *nesmí vyskytovat nikd předchozích řádcích*. K němu do řádku doplníme příslušné součty. Tak po pujeme dále, až vytvoříme tabulku s $2^{(n-k)}$ řádky.

První řádek tabulky obsahuje lineární prostor K, druhý řádek tab obsahuje množinu $K+\boldsymbol{e}_2$, která je podle věty ?? disjunktní s K. Platí t $\boldsymbol{e}_2 \notin K$. Třetí řádek obsahuje množinu $K+\boldsymbol{e}_3$, která je disjunktní s K i s K- protože $\boldsymbol{e}_3 \notin K$ a $\boldsymbol{e}_3 \notin K+\boldsymbol{e}_2$, takže můžeme dvakrát použít větu ??. A dále. Slova v jednom řádku jsou samozřejmě různá. Máme tedy zaručeno žádné slovo se v tabulce neopakuje a že jsou vyčerpána všechna slova pros $\mathbf{Z}_2^n$.

Pokud nyní dekodér přijme slovo $\boldsymbol{w}$, vyhledá ho v tabulce. Například s našel na i-tém řádku tabulky. Dekodér na základě toho rozhodne, že doš chybě $\boldsymbol{e}_i$ a opraví ji tak, že provede $\boldsymbol{w}-\boldsymbol{e}_i$. (Místo odčítání může vyko $\boldsymbol{w}+\boldsymbol{e}_i$, protože v aritmetice $\mathbf{Z}_2$ to dopadne stejně). Pokud $\boldsymbol{w}$ bylo na j- sloupci tabulky, dekodér se tímto postupem vrací ke kódovému slovu $\boldsymbol{v}_j$.

Aby dekodér nemusel prohledávat celou tabulku o 2^n slovech, vyp nejdříve syndrom přijatého vektoru: $\boldsymbol{s}^T = \mathbf{H}\cdot\boldsymbol{w}^T$. Vlevo od svislé čáry syndromy všech slov, které jsou napsány vpravo na stejném řádku (viz věta Prohledáním tabulky syndromů a porovnáním se syndromem slova $\boldsymbol{w}$ deko odhalí správně řádek tabulky, ve kterém slovo $\boldsymbol{w}$ leží. Dekodér tedy nen pracovat s celou tabulkou, ale jen se sloupcem syndromů a sloupcem chybov slov.

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 obdr nekódového slova opraví první bit. Kdybychom zvolili jiné chybové slovo (n 0100), dostaneme jinou tabulku: druhý řádek bude obsahovat slova v ji pořadí. Dekodér podle takové pozměněné tabulky bude po přijetí nekódov slova opravovat jiný bit. Bohužel, nemáme žádnou záruku, že dekodér op správný bit. Tabulka určuje pevně jeden bit, který bude dekodér opravo Lepší by bylo, kdybychom v prvním sloupci s chybovými slovy měli zaps všechna chybová slova tvaru 1000, 0100, 0010, 0001. To bychom ale potřebo mít v tabulce pět řádků a ne jen dva. Dva řádky v tabulce jsou důsledkem t že kód pracuje jen s jedním kontrolním bitem a že $2^1 = 2$. Můžeme tedy že pro úspěšnou opravu chyb je jeden kontrolní bit málo. To ostatně čl 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	11
100	100000	000100	110010	101001	010110	111011	001101	01
010	010000	110100	000010	011001	100110	001011	111101	10
001	001000	101100	011010	000001	111110	010011	100101	11
110	110000	010100	100010	111001	000110	101011	011101	00
101	101000	001100	111010	100001	011110	110011	000101	01

Jestliže předpokládáme, že přijaté slovo obsahuje jednu chybu, pak v uvedená oprava nemusí být jediná možná. Opravou posledního bitu ve s 111110 také dostáváme kódové slovo 111111. Problém tohoto kódu z poh tabulky pro opravování chyb je, že chybová slova s jednou jedničkou se ob dvě na společném řádku tabulky. Na dalších řádcích (za čtvrtým řádkem nemůžeme použít chybové slovo 000001, protože toto slovo se na čtvrtém řá už objevilo. Pokud bychom na čtvrtém řádku použili chybové slovo 000001, by se na tomto řádku zase vyskytlo i 001000. Množina slov vedle konkrét syndromu se totiž nemůže změnit, protože se jedná o množinu řešení sous $\mathbf{H}\boldsymbol{x}^T = \boldsymbol{s}^T$. Takže bychom dostali sice jinou tabulku pro opravování c ale chybová slova s jednou jedničkou by se ani tak nepodařilo oddělit do notlivých řádků. Ačkoli (na rozdíl od kódu s kontrolním bitem parity) m v tabulce dostatečný počet řádků, nemáme možnost dostat všechna chyb slova s jednou jedničkou do prvního sloupce tabulky. Dokonce jsme nucen posledním řádku tabulky použít chybové slovo se třemi jedničkami.

[podminkykodu] Nezdary při opravování chyb v předchozím příkladě inspirují k formulaci podmínek na kód, který spolehlivě opravuje jednu ch

Předpokládáme lineární (n, k) kód. Chybových slov s jednou jedničko n a potřebujeme je všechna rozmístit do prvního sloupce tabulky pro opr vání chyb. Žádná jiná chybová slova se v tomto sloupci nesmějí objevit. Z t vyplývá, že počet řádků tabulky musí být $n + 1$ (první řádek tabulky o huje samotný kód). Protože počet řádků tabulky je $2^{(n-k)}$, máme podmí $2^{(n-k)} = n + 1$. Označíme-li počet kontrolních bitů $c = n - k$, pak je uve podmínka asi lépe čitelná ve tvaru $n = 2^c - 1$. Celkový počet bitů n tedy m být o jedničku menší než mocnina dvojky a hodnota této mocniny udává čet kontrolních bitů. Postupně pro $c = 2, 3, 4, 5, 6, \ldots$ dostáváme (3,1), ((15,11), (31,26), (63,57), . . . kódy.

Abychom mohli rozmístit všechna chybová slova s jednou jedničkou do ního sloupce, potřebujeme ještě zaručit, že žádné slovo s jednou jedničkou

Důkaz. Stačí si uvědomit, že syndrom slova s jednou jedničkou na i-tém m
je roven i-tému sloupci kontrolní matice. To vyplývá z maticového násob
$\mathbf{H} \cdot \boldsymbol{w}^T = \boldsymbol{s}^T$.

Aby lineární (n, k) kód opravoval všechny jednoduché chyby ve slov
podle poznámky ?? nutné, aby $n = 2^c - 1$, kde $c = n - k$, a dále podle vět
je nutné, aby kontrolní matice neměla žádný sloupec nulový a všechny slou
od sebe vzájemně různé. Těch sloupců musí být $n = 2^c - 1$, a přitom v
sloupce je c. Z toho nám vyplývá jediný možný tvar kontrolní matice (a
pořadí sloupců): v jednotlivých sloupcích kontrolní matice napíšeme ve d
kové soustavě všechna čísla $1, 2, 3, \ldots, n$. Lineárnímu kódu s takovou kontr
maticí říkáme *Hammingův kód*.

[hamming74] Ukážeme si Hammingův $(7, 4)$ kód. Podle předchozí pozná
napíšeme ve dvojkové soustavě do sloupců kontrolní matice čísla 1,2,3,4,5,

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

Syndromy a první sloupec tabulky pro opravování chyb napíšeme (kvůli úsp
místa v tomto textu) místo do sloupců do řádků:

	001	010	011	100	101	110
00	1000000	0100000	0010000	0001000	0000100	0000010

Vidíme, že při této volbě pořadí sloupců kontrolní matice má dek
výrazně usnadněnou práci: nemusí prohledávat v tabulce syndromů, aby zj
odpovídající chybové slovo. Stačí, aby interpretoval syndrom jako číslo zaps
ve dvojkové soustavě. Toto číslo udává pozici bitu chybového slova, kd
nalézá jednička.

stejného kódu (poznámka ??):

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \sim$$

Podle věty ?? se tedy jedná o systematický kód, protože $\mathbf{H}' = (\mathbf{C}^T|\mathbf{E}')$. P
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 výstup
další tři kontrolní bity $\boldsymbol{v}'$ počítáme ze vstupního slova $\boldsymbol{u}$ podle poznámky

$$\boldsymbol{v}' = \boldsymbol{u} \cdot \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

Analogicky se postupuje při návrhu $(15, 11)$, $(31, 26)$, $(63, 57)$ atd. H
mingových kódů. Všimněte si, že s rostoucím n se výrazně zlepšuje poměr in
mačních bitů ku celkovému počtu přenášených bitů. To je pro uživatele, kte
zajímají jen o informační bity, dobrá zpráva. Ovšem prodlužováním délky
nášených slov se zase zvyšuje pravděpodobnost výskytu více než jedné ch
ve slově. Dekodér Hammingova kódu v takovém případě selže.

Ve výpočetní technice se pracuje s přenosy 8 bitů, 16 bitů, 32 bitů
Hammingův kód předpokládá přenos slov délky o jeden bit kratší. Co se zby
bitem? Použijeme jej pro kontrolu parity. Tím dostáváme *rozšířený Hammin*
kód, který umožní spolehlivě opravit jednu chybu a detekovat chyby dvě.

Tento kód umí opravit jednu chybu ve slově a detekovat chyby dvě. Jak deko
může postupovat? Přijme slovo $\boldsymbol{w}$ a vypočte syndrom $\boldsymbol{s}^T = \mathbf{H} \cdot \boldsymbol{w}^T$. Je-li
drom nulový vektor, je slovo $\boldsymbol{w}$ kódové a dekodér nic neopravuje. Jsou-li p
tři bity syndromu nulové a poslední nenulový, došlo při přenosu jen k ch
posledního kontrolního bitu parity. Je-li na prvních třech pozicích syndr
aspoň jeden bit nenulový a poslední bit syndromu je rovněž nenulový, doš
lichému počtu chyb ve slově. Dekodér předpokládá, že došlo k jediné chyb
podle prvních třech bitů syndromu zjistí, který bit ve slově má opravit (st
jako v příkladu ??). Je-li konečně poslední bit syndromu nulový, ale synd
obsahuje aspoň jeden nenulový bit, pak došlo k sudému počtu chyb. T
počet chyb neumí dekodér opravit, ale detekuje tento stav jako dvojnásob
chybu.

Všimněte si, že nejmenší Hammingova vzdálenost mezi dvěma slovy r
řeného Hammingova kódu je 4. To je v souladu s výsledky příkladu ??.

17. Literatura

[1] J. Adámek, *Foundations of Coding.* A Wiley-Interscience publication, N York 1991.

[2] V. Bartík, *Úvod do algebry.* Text k přednášce 1996 na http://math.fel

[3] H.–J. Bartsch, *Matematické vzorce.* Academia, Praha 2006 (4. vydání

[4] R. A. Beezer, *A First Course in Linear Algebra.* Tacoma, Washing 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) 1 Existuje slovenský překlad staršího vydání *Prehľad modernej algebry*, A Bratislava, 1979.

[7] Don Coppersmith and Shmuel Winograd. *Matrix multiplication via thmetic progressions.* Journal of Symbolic Computation, 9:251?280, 1

[8] M. Demlová, B. Pondělíček, *Úvod do algebry.* Vydavatelství ČVUT, Pr 1996.

[9] M. Dont, *Elementy numerické lineární algebry.* Vydavatelství ČVUT, P 2004.

[10] I. M. Gelfand, *Lineární algebra.* Překlad M. Fiedler, ČSAV, Praha 19

[11] J. Hefferon, *Linear Algebra.* Colchester, Vermont USA, volně dostupné http://joshua.smcvt.edu/linearalgebra/.

[12] S. Jílková, V. Maňasová, Z. Tischerová, *Lineární algebra – úlohy.* Vyd telství ČVUT, Praha 1987.

[13] A. Kalousová, *Skripta z algebry.* Text volně dostupný například

[17] V. Mahel & kol. kat. matematiky, *Sbírka úloh z lineární algebry a analyt geometrie.* Vydavatelství ČVUT, Praha 1986.

[18] J. Matoušek, *Šestnáct miniatur.* Volně dostupný text s aplikacemi line algebry tam, kde bychom to možná nečekali, http://kam.mff.cuni.cz

[19] L. Motl, M. Zahradník, *Pěstujeme lineární algebru.* MFF UK, Praha (skriptum přístupné na http://www.kolej.mff.cuni.cz/~lmotm275/

[20] P. Olšák, *Úvod do algebry, zejména lineární.* FEL ČVUT, Praha 200

[21] P. Olšák, *TEXbook naruby.* Konvoj, Brno 2001 (2. vydání). Text v 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 Na Moskva 1970.

[24] P. Pták, *Introduction to Linear Algebra.* Vydavatelství ČVUT, Praha 2

[25] K. Rektorys, *Přehled užité matematiky.* Prometheus, Praha 2003 (6. dání).

[26] P. Vopěnka, *Úhelný kámen evropské vzdělanosti a moci – rozpravy s metrií.* Práh, Praha 2003.

[27] K. Výborný, M. Zahradník & kol. *Sbírka příkladů z lineární algebry.* V dostupný text k nalezení například na http://www.kolej.mff.cuni.c

[28] J. Žára, B. Beneš, J. Sochor, P. Felkel, *Moderní počítačová grafika.* C puter Press, 2005 (2. vydání).