Petr Olšák

Lineární algebra

Praha, 2000-2007

Verze textu: 31. 7. 2007

Poznámka ke změnám v textu. V září 2006 jsem původní text rozšířil o mnoho nových partií, protože se změnily osnovy algebry pro první ročník otevřením programu STM na naší fakultě. Veškerý nový text jsem připojoval na konce stávajících kapitol, abych zachoval číslování definic a vět původního textu. Na konec první kapitoly o lineárních prostorech jsem připojil text o grupách a tělesech. Na konec druhé kapitoly (o obalech a bázích) jsem vložil Steinitzovu větu o výměně. Na konci kapitoly o maticích přibyly věty o hodnosti součinu matic. Na konec kapitoly o soustavách lineárních rovnic jsem přidal několik dodatků na postupy řešení soustav. Na konec kapitoly o lineárních zobrazeních jsem připojil definici pojmu vlastní číslo a vlastní vektor včetně povídání o základních vlastnostech, jako například podobnost s diagonální maticí. Na konec textu jsem připojil zcela novou kapitolu 10 obsahující úvod do kódování.

V červnu 2007 jsem tento text použil ve skriptech [18]. Tam je navíc ke každé kapitole připojena rozsáhlá sbírka cvičení a je přidána kapitola o polynomech. Tyto věci ve verzi volně šířené na internetu nejsou. Zdrojový text volně šířeného textu i skript je společný (veřejně vystavený soubor `linal.tex`). Překlad textu TEXem se při zpracování skript a internetové verze liší jen na několika místech (viz přepínač `\ifbook`). Při tisku skript se pochopitelně odkazuje na další zdrojové soubory, které nejsou na internetu zveřejněny. Korektury, které jsem zapracoval při vydání skript, jsou zaneseny i do této verze volně šířeného textu. Změnil jsem značení pro lineární obal řádků matice a dále skládání zobrazení ($\circ$) v nové verzi textu čteme zprava doleva. Při výrobě skript vznikl též seznam literatury a rejstřík, což jsou věci, které jsem nově zařadil i do internetové verze textu.

Obsah

Gaussova eliminační metoda

Než se pustíme do studia lineárních prostorů a podprostorů, závislosti a nezávislosti vektorů, bází a lineárních obalů, uvedeme si v této úvodní kapitole metodu, která se nám bude často hodit. Protože se k řešení soustav vrátíme podrobněji v kapitole páté, řekneme si zde jen to nejnutnější a budeme se v některých případech vyjadřovat možná poněkud těžkopádně. Vše napravíme v kapitole 5.

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

Úvodní příklad

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

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

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

$$\begin{array}{llll} 2x - 5y = 16 & & \Rightarrow\ 2(2y+7) - 5y = 14 - y = 16 \ \Rightarrow\ \underline{y = -2} & \\ -x + 2y = -7 \ \Rightarrow & x = 2y + 7 & & \Rightarrow\ x = 2(-2) + 7 \underline{= 3}, \end{array}$$

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

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

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

$$\begin{aligned} 2x - 5y &= 16 \\ -x + 2y &= -7 \end{aligned} \sim \begin{aligned} 2x - 5y &= 16 \\ -2x + 4y &= -14 \end{aligned} \sim \begin{aligned} 2x - 5y &= 16 \\ 0x - y &= 2 \end{aligned} \sim \begin{aligned} 2x - 5y &= 16 \\ y &= -2 \end{aligned} \sim \begin{aligned} 2x + 0y &= 6 \\ y &= -2 \end{aligned} \sim \begin{aligned} x &= 3 \\ y &= -2 \end{aligned}$$

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

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

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

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

$$\left(\begin{array}{rr|r} 2 & -5 & 16 \\ -1 & 2 & -7 \end{array}\right) \sim \left(\begin{array}{rr|r} 2 & -5 & 16 \\ -2 & 4 & -14 \end{array}\right) \sim \left(\begin{array}{rr|r} 2 & -5 & 16 \\ 0 & -1 & 2 \end{array}\right) \sim \left(\begin{array}{rr|r} 2 & -5 & 16 \\ 0 & 1 & -2 \end{array}\right) \sim \left(\begin{array}{rr|r} 2 & 0 & 6 \\ 0 & 1 & -2 \end{array}\right) \sim \left(\begin{array}{rr|r} 1 & 0 & 3 \\ 0 & 1 & -2 \end{array}\right)$$

Další příklad

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

Máme řešit následující soustavu lineárních rovnic

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Pokud bychom se rozhodli například z první rovnice počítat x_2, pak by neznámá x_1 mohla nabývat libovolných hodnot a výsledek by byl formálně zapsán poněkud jinak: $x_1 = w$, $x_2 = -8 + 2u + 2w$, $x_3 = -4 - u$, $x_4 = 1 + 2u$, $x_5 = u$, $u \in \mathbf{R}$, $w \in \mathbf{R}$. Vidíme tedy, že neexistuje jednoznačný zápis výsledku. Oba zápisy popisují stejnou množinu řešení, každý trochu jiným způsobem.

Popis metody

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

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

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

K1. Řádky 1 až r opíšeme beze změny.
K2. K řádku $r+1$ přičítáme $(-b_1/a)$ násobek řádku r, k řádku $r+2$ přičítáme $(-b_2/a)$ násobek řádku r, atd., až konečně k řádku poslednímu přičítáme $(-b_k/a)$ násobek řádku r.

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

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

G1. Nastavíme $r = 1$, $s = 1$.
G2. Nechť a je prvek matice z s-tého sloupce a r-tého řádku. Pokud je $a = 0$ a všechny prvky pod prvkem a v s-tém sloupci jsou také nulové, zvětšíme s o jedničku a opakujeme krok G2.
G3. Je-li $a = 0$, a přitom existuje nenulový prvek pod prvkem a v s-tém sloupci na řádku r_1, prohodíme řádek r s řádkem r_1. Od této chvíle je v nové matici prvek na r-tém řádku a s-tém sloupci nenulový.
G4. Vytvoříme nuly pod nenulovým prvkem a z r-tého řádku a s-tého sloupce způsobem, popsaným v krocích K1 a K2.
G5. Existují-li v matici řádky celé nulové, z matice je odstraníme.
G6. Zvětšíme r o jedničku a s o jedničku a celou činnost opakujeme od kroku G2 znova.

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

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

Diskuse po převedení matice

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

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

soustava nemá řešení. Tento řádek totiž odpovídá rovnici

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

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

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

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

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

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

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

Příklad, kdy soustava nemá řešení

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

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

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

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

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

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

1. Lineární prostor, grupa, těleso

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

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

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

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

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

Pro matematické sdělení nových poznatků je obvykle členění textu na definice, věty a důkazy dostačující. V této učebnici si navíc budeme ilustrovat novou problematiku na *příkladech* a občas prohodíme nějakou *poznámku.* Dokladem toho je i tato poznámka 1.1.

1.2. Poznámka. V následující definici lineárního prostoru 1.6 se pracuje s množinami blíže nespecifikovaných objektů. Jediné, co s těmi objekty umíme dělat, je vzájemně objekty sčítat a násobit objekt reálným číslem. Přitom tyto operace (sčítání a násobení reálným číslem) je potřeba pro konkrétní množiny objektů definovat. Pro každou množinu objektů mohou tyto operace vypadat jinak. Skutečnost, že není řečeno, jak objekty a operace s nimi konkrétně vypadají, může být pro některé čtenáře poněkud frustrující. Proto před definicí uvedeme příklady množin objektů, které lze sčítat a násobit konstantou.

1.3. Příklad. Nechť $\mathbf{R}^2$ je množina všech uspořádaných dvojic reálných čísel, tj. $\mathbf{R}^2 = \{(a,b); a \in \mathbf{R}, b \in \mathbf{R}\}$ (symbolem $\mathbf{R}$ označujeme reálná čísla, složky uspořádané dvojice píšeme do kulatých závorek a oddělujeme čárkou). Definujme sčítání dvou uspořádaných dvojic:

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

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

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

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

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

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

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

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

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

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

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

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

$$p(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\quad (a_n,a_{n-1},\ldots,a_1,a_0 \text{ jsou nějaká reálná čísla}). \tag{1.5}$$

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

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

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

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

1.5. Poznámka. V předchozích dvou příkladech jsme definovali na množině nějakých objektů sčítání a násobení reálným číslem. Pro větší přehlednost jsme nově definované operace zapisovali do kroužku, abychom je odlišili od operací sčítání a násobení reálných čísel. To ale není potřeba. Stačí používat tytéž znaky, protože podle typu objektů, které do operace vstupují, okamžitě poznáme, jakou operaci máme použít (zda nově definovanou nebo známou operaci na reálných číslech). Takové automatické přizpůsobení operace podle typu operandů znají programátoři objektově orientovaných jazyků. Tam se tomu říká „přetěžování operátorů“.

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

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

1.6. Definice. *Lineárním prostorem* nazýváme každou neprázdnou množinu L, na které je definováno sčítání $+\colon L\times L\to L$ a násobení reálným číslem $\cdot\colon \mathbf{R}\times L\to L$ a tyto operace splňují pro každé $\boldsymbol{x}\in L,\boldsymbol{y}\in L,\boldsymbol{z}\in L,\alpha\in\mathbf{R},\beta\in\mathbf{R}$ vlastnosti: *Definice lineárního prostoru*

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

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

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

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

Důkaz. Použijeme vlastnosti z definice 1.6. Pro přehlednost píšeme nad rovnítka číslo použité vlastnosti.

$$
\begin{array}{ll}
(1) & \boldsymbol{x} + \boldsymbol{o} \overset{(7)}{=} \boldsymbol{x} + 0 \cdot \boldsymbol{x} \overset{(6)}{=} 1 \cdot \boldsymbol{x} + 0 \cdot \boldsymbol{x} \overset{(5)}{=} (1+0) \cdot \boldsymbol{x} = 1 \cdot \boldsymbol{x} \overset{(6)}{=} \boldsymbol{x}. \\
(2) & \alpha \cdot \boldsymbol{o} \overset{(7)}{=} \alpha \cdot (0 \cdot \boldsymbol{x}) \overset{(3)}{=} (\alpha \cdot 0) \cdot \boldsymbol{x} = 0 \cdot \boldsymbol{x} \overset{(7)}{=} \boldsymbol{o}. \\
(3) & \boldsymbol{x} \overset{(6)}{=} 1 \cdot \boldsymbol{x} = \left(\frac{1}{\alpha}\,\alpha\right) \cdot \boldsymbol{x} \overset{(3)}{=} \frac{1}{\alpha} \cdot (\alpha \cdot \boldsymbol{x}) \overset{\text{(z předpokladu)}}{=} \frac{1}{\alpha} \cdot \boldsymbol{o} \overset{\text{(vlastnost (2) věty 1.7)}}{=} \boldsymbol{o}.
\end{array}
$$

1.8. Poznámka. Ve vlastnostech (1) až (7) v definici 1.6 se pracuje se znaky „+“ a „·“ v souladu s poznámkou 1.5 ve dvojím významu. Buď to jsou operace s prvky množiny L nebo operace s reálnými čísly. Například ve vlastnosti (5) je první symbol „+“ použit ve významu sčítání na množině reálných čísel, zatímco druhý symbol „+“ je použit ve významu sčítání na množině L. Jako cvičení zkuste o každé použité operaci ve vzorcích (1) až (7) rozhodnout, jakého je druhu.

1.9. Příklad. Ukážeme, že množina $\mathbf{R}^2$ z příkladu 1.3 se sčítáním a násobením skalárem podle definic (1.1) a (1.2) tvoří lineární prostor. Místo znaků „$\oplus$“ a „$\odot$“ budeme nadále používat znaky „+“ a „·“. *Prostor* $\mathbf{R}^2$

Nejprve je třeba zjistit, zda operace „+“ a „·“ jsou skutečně definovány způsobem, jak požaduje definice 1.6, tj. zda platí $+ : \mathbf{R}^2 \times \mathbf{R}^2 \to \mathbf{R}^2$ a $\cdot : \mathbf{R} \times \mathbf{R}^2 \to \mathbf{R}^2$. To jsme ale už ověřili dříve, viz (1.3).

Dále zjistíme platnost vlastností (1) až (7) z definice 1.6. Vlastnost (1) jsme podrobně ověřovali v příkladu 1.3. Pokračujeme tedy vlastností (2). Pro každé $a, b, c, d, e, f \in \mathbf{R}$ platí:

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

Při úpravách jsme nejprve dvakrát použili definici (1.1), pak jsme v jednotlivých složkách využili toho, že pro sčítání reálných čísel platí asociativní zákon a konečně jsme zase dvakrát použili definici (1.1). Nyní dokážeme další vlastnosti. Pro každé $a, b, c, d, \alpha, \beta \in \mathbf{R}$ platí:

$$
\begin{array}{ll}
(3) & \alpha \cdot \big(\beta \cdot (a,b)\big) = \alpha \cdot \big(\beta\, a, \beta\, b\big) = \big(\alpha\,(\beta\, a), \alpha\,(\beta\, b)\big) = \big((\alpha\,\beta)\, a, (\alpha\,\beta)\, b\big) = (\alpha\,\beta)\,(a,b), \\
(4) & \alpha \cdot \big((a,b) + (c,d)\big) = \alpha \cdot (a+c, b+d) = \big(\alpha\,(a+c), \alpha\,(b+d)\big) = (\alpha\, a + \alpha\, c, \alpha\, b + \alpha\, d) = \\
& \qquad = (\alpha\, a, \alpha\, b) + (\alpha\, c, \alpha\, d) = \alpha\,(a,b) + \alpha\,(c,d), \\
(5) & (\alpha+\beta) \cdot (a,b) = \big((\alpha+\beta)\, a, (\alpha+\beta)\, b\big) = (\alpha\, a + \beta\, a, \alpha\, b + \beta\, b) = (\alpha\, a, \alpha\, b) + (\beta\, a, \beta\, b) = \\
& \qquad = \alpha\,(a,b) + \beta\,(a,b), \\
(6) & 1 \cdot (a,b) = (1\, a, 1\, b) = (a,b), \\
(7) & \text{dvojice } (0,0) \text{ splňuje: } (0,0) = 0 \cdot (a,b), \text{protože } 0 \cdot (a,b) = (0\, a, 0\, b) = (0,0).
\end{array}
$$

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

Vidíme, že nulovým vektorem lineárního prostoru $\mathbf{R}^2$ je dvojice $(0,0)$. Podle konvence ze závěru definice 1.6 jsme oprávněni uspořádaným dvojicím se sčítáním a násobením podle definic (1.1) a (1.2) říkat vektory.

1.10. Příklad. Množina $\mathbf{R}^2$ se sčítáním $\oplus$ podle definice (1.4) a násobením $\odot$ podle (1.2) netvoří lineární prostor. Není totiž splněna například vlastnost (1) z definice 1.6.

Prostor $\mathbf{R}^n$

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

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

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

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

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

Důkaz bychom provedli analogicky jako v příkladu 1.9, ale pro úsporu místa to již nebudeme opakovat. Vidíme tedy, že uspořádané n-tice s takto definovaným sčítáním a násobením skalárem můžeme nazývat vektory. Speciálně v případě uspořádaných n-tic mluvíme o *aritmetických vektorech.* Číslo a_i nazýváme i-tou složkou vektoru $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$.

1.12. Příklad. Množina $\mathbf{R}$ s obvyklým sčítáním reálných čísel a násobení reálného čísla reálným číslem tvoří lineární prostor. To je zřejmé. Sčítání a násobení reálných čísel totiž splňuje vlastnosti (1) až (7) z definice 1.6. Tento poznatek si jistě přinášíte ze střední školy. V tomto textu jsme jej už použili, když jsme ověřovali, že $\mathbf{R}^2$ nebo $\mathbf{R}^n$ je lineární prostor.

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

Prostor funkcí

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

$$(f + g)(x) \stackrel{\text{df}}{=} f(x) + g(x) \qquad \forall x \in D \tag{1.6}$$
$$(\alpha \cdot f)(x) \stackrel{\text{df}}{=} \alpha\, f(x) \qquad \forall x \in D \tag{1.7}$$

(srovnejte s definicí $\oplus$ a $\odot$ v příkladu 1.4). Ukážeme, že množina F_D s takto definovaným sčítáním a násobením skalárem tvoří lineární prostor.

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

Dále potřebujeme ověřit vlastnosti (1) až (7) z definice 1.6. Pro libovolné $f \in F_D, g \in F_D, h \in F_D$, $\alpha \in \mathbf{R}, \beta \in \mathbf{R}$ a pro všechna $x \in D$ platí:

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

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

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

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

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

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

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

Ačkoli tyto vzorce vypadají na první pohled jen jako „hraní se závorkami", musíme si uvědomit, že rovnost funkcí zde dokazujeme na základě rovnosti jejich hodnot v každém bodě $x \in D$ a že při důkazu používáme nejprve rozepsání operací podle definic (1.6) a (1.7). Tím problém převádíme na sčítání a násobení reálných čísel, kde jsou vlastnosti (1) až (7) zaručeny. Jako cvičení si zkuste přepsat tyto vzorce tak, že odlišíte operace sčítání funkcí a násobení funkce skalárem od běžných operací „+" a „·" pro reálná čísla. Použijte například symbolů $\oplus$ a $\odot$, jako v příkladu 1.4.

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

1.14. Příklad. Ukážeme, že množina P všech polynomů s definicemi sčítání a násobení skalárem podle příkladu 1.4 tvoří lineární prostor. *Prostor polynomů*

Především součet dvou polynomů je polynom a skalární násobek polynomu je polynom, takže platí, že $+: P \times P \to P$ a $\cdot: \mathbf{R} \times P \to P$. To je ale vše, co potřebujeme dokázat. Ověřováním vlastností (1) až (7) se nemusíme zdržovat, protože jsme definice sčítání a násobení polynomů převzali z prostoru funkcí F_D, o němž jsme dokázali v příkladu 1.13, že se jedná o lineární prostor (volíme $D = \mathbf{R}$). Při ověřování vlastností (1) až (7) bychom dělali vlastně to samé jako v příkladu 1.13, jen na podmnožině $P \subseteq F_D$.

1.15. Příklad. Nechť $n \in \mathbf{N}$, $n \geq 0$ (symbolem $\mathbf{N}$ značíme množinu přirozených čísel). Množina P_n všech polynomů právě n-tého stupně s definicemi sčítání a násobení skalárem podle příkladu 1.4 *netvoří* lineární prostor. Připomeneme, že *stupeň polynomu* se definuje jako největší $k \in \mathbf{N}$ takové, že a_k je ve vzorci (1.5) nenulové. Jsou-li všechna a_k nulová, definujeme stupeň takového polynomu jako -1.

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

1.16. Poznámka. Příklady 1.14 a 1.15 ukazují, že můžeme vymezit podmnožinu $M \subseteq L$ lineárního prostoru L a převzít pro ni operace sčítání a násobení konstantou z L. Za jistých okolností množina M s převzatými operacemi může být lineárním prostorem, ale nemusí být vždy. Z příkladu 1.14 navíc vidíme, že stačí ověřit vlastnosti $+: M \times M \to M$ a $\cdot: \mathbf{R} \times M \to M$, abychom mohli prohlásit, že M je lineární prostor. Vlastnosti (1) až (7) není třeba znovu ověřovat. Podmožinu lineárního prostoru, která je sama lineárním prostorem při použití stejných operací, nazýváme lineárním podprostorem. Přesněji viz následující definice.

1.17. Definice. Nechť L je lineární prostor s operacemi „+“ a „·“. Neprázdnou množinu $M \subseteq L$ nazýváme *lineárním podprostorem prostoru* L, pokud pro všechna $\boldsymbol{x} \in M, \boldsymbol{y} \in M$ a $\alpha \in \mathbf{R}$ platí: *Lineární podprostor*

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

1.18. Příklad. Množina všech polynomů P z příkladu 1.14 je lineárním podprostorem množiny všech funkcí F_D z příkladu 1.13, kde volíme $D = \mathbf{R}$. Množina P_n všech polynomů právě n-tého stupně z příkladu 1.15 není lineárním podprostorem lineárního prostoru F_D ani lineárního prostoru P.

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

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

Stačí pro množinu M dokázat vlastnosti (1) a (2) z definice 1.17. Platí (1) součet dvou uspořádaných n-tic, ve kterých se složky rovnají, je uspořádaná n-tice, ve kterých se složky rovnají. (2) vynásobením uspořádané n-tice, ve které se složky rovnají, reálným číslem, dostáváme zase uspořádanou n-tici, ve které se složky rovnají.

1.21. Příklad. Uvažujme množiny $M \subseteq \mathbf{R}^3$, $N \subseteq \mathbf{R}^3$ a $S \subseteq \mathbf{R}^3$, které jsou 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 $\mathbf{R}^3$, zatímco S není lineárním podprostorem lineárního prostoru $\mathbf{R}^3$.

Ověříme vlastnost (1) z definice 1.17: Nechť $(x_1, y_1, z_1) \in M$ a $(x_2, y_2, z_2) \in M$. Pak platí $x_1 + 2y_1 = 0$ a $x_2 + 2y_2 = 0$. Pro součet $(x_1 + x_2, y_1 + y_2, z_1 + z_2)$ platí $x_1 + 2y_1 + x_2 + 2y_2 = 0$ (sečetli jsme předchozí rovnice), tj. $(x_1 + x_2) + 2(y_1 + y_2) = 0$, takže i součet leží v množině M. Nyní vlastnost (2): Jestliže $(x, y, z) \in M$, $\alpha \in \mathbf{R}$, pak platí $x + 2y = 0$. Vynásobením rovnice číslem α dostáváme, že též $\alpha\, x + 2\alpha\, y = 0$, což ale znamená, že i trojice $\alpha \cdot (x, y, z)$ leží v množině M. Ověření, že množina N je lineárním podprostorem, lze provést podobně.

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

Průnik prostorů

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

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

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

Důkaz. (1) Z předpokladů věty a definice 1.17 víme, že pro $\boldsymbol{x} \in M$, $\boldsymbol{y} \in M$, $\alpha \in \mathbf{R}$ je $\boldsymbol{x} + \boldsymbol{y} \in M$ a $\alpha \cdot \boldsymbol{x} \in M$. Totéž platí pro množinu N. Pokud nyní $\boldsymbol{x} \in M \cap N$, $\boldsymbol{y} \in M \cap N$, pak $\boldsymbol{x}$ i $\boldsymbol{y}$ leží současně v M i N, takže platí, že $\boldsymbol{x} + \boldsymbol{y} \in M$, $\alpha \cdot \boldsymbol{x} \in M$ a současně $\boldsymbol{x} + \boldsymbol{y} \in N$, $\alpha \cdot \boldsymbol{x} \in N$. Prvky $\boldsymbol{x} + \boldsymbol{y}$ a $\alpha \cdot \boldsymbol{x}$ leží v obou množinách M a N současně a to není jinak možné, než že leží v průniku těchto množin.

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

1.23. Příklad. Uvažujme podprostory M a N z příkladu 1.21. Podle věty 1.22 je také $M \cap N$ lineárním podprostorem lineárního prostoru $\mathbf{R}^3$.

Prostor orientovaných úseček

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

Definujme nyní sčítání $+ : U_O \times U_O \to U_O$ ryze konstruktivně takto: Úsečky $\boldsymbol{u} \in U_O$, $\boldsymbol{v} \in U_O$ doplníme na rovnoběžník. Úhlopříčku, která začíná v bodě O a končí v protějším bodě rovnoběžníka, prohlásíme za součet úseček $\boldsymbol{u}$ a $\boldsymbol{v}$, tedy $\boldsymbol{u} + \boldsymbol{v}$. Dále definujme násobení skalárem $\cdot : \mathbf{R} \times U_O \to U_O$ takto: změříme nějakým měřítkem (pracujeme pořád se stejným měřítkem, jedno jakým) velikost úsečky $\boldsymbol{u}$. Tím dostáváme nezáporné reálné číslo. Toto číslo vynásobíme skalárem α a výsledek násobení označme písmenem $c \in \mathbf{R}$. Je-li $c > 0$, naneseme výslednou úsečku $\alpha \cdot \boldsymbol{u}$ na stejnou polopřímku, na které leží $\boldsymbol{u}$ a velikost má c. Je-li $c < 0$, naneseme výslednou úsečku $\alpha \cdot \boldsymbol{u}$ na opačnou polopřímku a velikost bude rovna $|c|$. Je-li $c = 0$ položme $\alpha \cdot \boldsymbol{u}$ rovnu degenerované úsečce, která začíná i končí v bodě O.

Množina U_O s takto konstruktivně definovaným sčítáním a násobením reálným číslem tvoří lineární prostor. Abychom toto tvrzení obhájili, musíme dokázat vlastnosti (1) až (7) z definice 1.6. (1) $\boldsymbol{u} + \boldsymbol{v} = \boldsymbol{v} + \boldsymbol{u}$, protože v obou případech doplňujeme na stejný rovnoběžník. (2) $(\boldsymbol{u} + \boldsymbol{v}) + \boldsymbol{w} = \boldsymbol{u} + (\boldsymbol{v} + \boldsymbol{w})$, protože postupné doplnění úhlopříčky rovnoběžníku $\boldsymbol{u}, \boldsymbol{v}$ a úsečky $\boldsymbol{w}$ na rovnoběžník vede ke stejnému výsledku, jako když nejprve sestavíme úhlopříčku rovnoběžníku $\boldsymbol{v}, \boldsymbol{w}$ a tu doplníme na rovnoběžník s úsečkou $\boldsymbol{u}$ (udělejte si náčtrek). (3) $\alpha \cdot (\beta \boldsymbol{u}) = (\alpha\, \beta) \cdot \boldsymbol{u}$, protože velikost těchto úseček je stejná (pro získání velikosti násobíme mezi sebou jen reálná čísla) a úsečky mají stejnou orientaci. (4) $\alpha \cdot (\boldsymbol{u} + \boldsymbol{v}) = \alpha \cdot \boldsymbol{u} + \alpha \cdot \boldsymbol{v}$, protože příslušné rovnoběžníky pro sčítání jsou podobné a druhý je α krát větší než první. Proto též jeho úhlopříčka bude α krát větší. (5) $(\alpha + \beta) \cdot \boldsymbol{u} = \alpha \cdot \boldsymbol{u} + \beta \cdot \boldsymbol{u}$, protože obě úsečky mají stejnou velikost a orientaci (pro získání velikosti násobíme a sčítáme reálná čísla). (6) $1 \cdot \boldsymbol{u} = \boldsymbol{u}$, protože obě úsečky mají stejnou velikost a orientaci. (7) $0 \cdot \boldsymbol{u}$ je vždy úsečka s nulovou velikostí, což je degenerovaná úsečka začínající i končící v bodě O. Ta je tedy nulovým prvkem našeho lineárního prostoru.

Vidíme, že orientované úsečky s výše definovaným geometrickým sčítáním a násobením skalárem můžeme v souladu s definicí 1.6 nazývat vektory. V kapitole deváté jim budeme říkat vázané vektory (vázané bodem O).

1.25. Příklad. Nechť $M \subset U_O$ jsou jen takové úsečky, které leží ve stejné rovině, jako leží náš papír, na který jsme v příkladu 1.24 nakreslili křížek. Vidíme, že $M \neq U_O$, protože například úsečka nenulové velikosti kolmá na náš papír neleží v M. Ukážeme, že množina M je lineární podprostor lineárního prostoru U_O. Skutečně, součet libovolných dvou úseček leží ve stejné rovině (protože tam leží celý rovnoběžník) a násobek úsečky leží dokonce na stejné přímce, jako původní úsečka, takže nutně zůstává ve stejné rovině.

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

Uvažujme nyní dvě roviny, které mají společný bod O, ale nejsou totožné. Jejich průnik je nějaká přímka, procházející bodem O. Všechny orientované úsečky z U_O, které leží v této přímce, tvoří podle věty 1.22 rovněž lineární podprostor lineárního prostoru U_O.

Triviální prostor

1.26. Poznámka. Zamysleme se, jak může vypadat lineární prostor s nejmenším počtem prvků. Podle definice 1.6 je lineární prostor vždy neprázdná množina, takže musí obsahovat aspoň jeden prvek. Ukazuje se, že jednobodová množina $L = \{\boldsymbol{o}\}$ je skutečně nejmenší možný lineární prostor. Přitom $\boldsymbol{o}$ je nulový prvek z vlastnosti (7). Sčítání je definováno předpisem $\boldsymbol{o} + \boldsymbol{o} \stackrel{\mathrm{df}}{=} \boldsymbol{o}$ a násobení skalárem α předpisem $\alpha \cdot \boldsymbol{o} \stackrel{\mathrm{df}}{=} \boldsymbol{o}$. Takový lineární prostor nazýváme *triviální*.

1.27. Poznámka. Ukážeme, že konečná množina obsahující aspoň dva prvky nemůže být lineárním prostorem. Znamená to, že se nám pro takovou množinu L nepovede najít operace $+ : L \times L \to L$ a $\cdot : \mathbf{R} \times L \to L$ takové, aby současně splňovaly vlastnosti (1) až (7) z definice 1.6.

Jeden z prvků množiny L musí být nulový prvek (označme jej $\boldsymbol{o}$) a jiný prvek označme třeba $\boldsymbol{x}$. Další prvky označovat nemusíme. Uvažujme množinu $K = \{\alpha \cdot \boldsymbol{x};\ \alpha \in \mathbf{R}\}$. Protože $K \subseteq L$, je i K konečná množina. Protože reálných čísel je nekonečně mnoho, a přitom K je konečná, musejí existovat dvě různá reálná čísla $\beta \neq \gamma$ taková, že $\beta \cdot \boldsymbol{x} = \gamma \cdot \boldsymbol{x}$. Z definice lineárního prostoru 1.6 dostáváme:

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

Nyní máme splněny předpoklady vlastnosti (3) věty 1.7 (volíme $\alpha = \gamma - \beta$). Dostáváme tedy $\boldsymbol{x} = \boldsymbol{o}$. To je ale spor s předpokladem, že jsme vybrali prvek $\boldsymbol{x}$ jiný než nulový. Konečná množina obsahující aspoň dva prvky tedy nemůže být lineárním prostorem.

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

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

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

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

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

Aby $\mathbf{R}^+$ s operacemi $\oplus$ a $\odot$ byl lineárním protorem, musí splňovat vlastnosti (1) až (7) z definice 1.6. Pro $x \in \mathbf{R}^+$, $y \in \mathbf{R}^+$, $z \in \mathbf{R}^+$, $\alpha \in \mathbf{R}$, $\beta \in \mathbf{R}$ je

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

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

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

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

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

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

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

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

1.29. Poznámka. Následující text až do konce kapitoly je poněkud abstraknější povahy. Přitom se jeho znalost nepředpokládá pro pochopení dalších kapitol. Pokud tedy čtenář nechce být hned v počátku studia zahlcen pojmy o algebraických strukturách, může tento text přeskočit.

1.30. Poznámka. Reálná čísla jsou množina prvků, které umíme vzájemně sčítat a vzájemně násobit. Přesněji, je to množina $\mathbf{R}$, na které jsou definovány obvyklé operace $+ : \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ a $\cdot : \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ s jistými vlastnostmi (asociativní zákon, distributivní zákon, atd.). Těmito vlastnostmi se budeme inspirovat a pokusíme se vybudovat abstraktní algebraickou strukturu, tzv. *těleso.* Jedním z možných konkrétních příkladů tělesa pak samozřejmě budou reálná čísla. Jenomže kromě nich budeme nacházet i jiné příklady těles. Začneme nejprve strukturou s jedinou operací.

1.31. Definice. Množinu G, na které je definována operace $\circ : G \times G \to G$ nazýváme *grupou*, pokud pro tuto operaci platí: *Grupa*

(1) $\forall x, y, z \in G : (x \circ y) \circ z = x \circ (y \circ z)$ (asociativní zákon),
(2) $\exists e \in G$, pro které platí $\forall x \in G : e \circ x = x \circ e = x$ (existence neutrálního/jednotkového prvku),
(3) $\forall x \in G\ \exists y \in G : x \circ y = y \circ x = e$ (existence opačného/inverzního prvku y pro každý prvek x).

Pokud navíc platí

(4) $\forall x, y \in G : x \circ y = y \circ x$ (komutativní zákon),

pak grupu G nazýváme *komutativní grupou.* Z historických důvodů a z úcty k norskému matematikovi, který rozpracoval teorii grup a bohužel zemřel mlád na zákeřnou nemoc ve věku 26 let, se komutativní grupa nazývá též *Abelova grupa.*

1.32. Poznámka. Niels Abel mimo jiné pomocí teorie grup dokázal, že nelze pro obecný polynom stupně vyššího než 4 najít vzorec na výpočet jeho kořenů z jeho koeficientů. Pro polynomy stupně 1, 2, 3 a 4 přitom takové vzorce existují. Pro stupeň 2 se jej žáci učí zpaměti: $x_{1,2} = (-b \pm \sqrt{b^2 - 4ac})/2a$.

1.33. Příklad. Jednoprvková množina $G = \{e\}$ s operací $e \circ e = e$ je nejmenší možnou grupou.

1.34. Příklad. Množina $\mathbf{R}$ s operací sčítání tvoří grupu. Skutečně platí asociativní zákon pro sčítání reálných čísel: $(x + y) + z = x + (y + z)$, dále existuje neutrální prvek 0, pro který $0 + x = x + 0 = 0$ a konečně pro každé $x \in \mathbf{R}$ existuje $y = -x$ tak, že $x + y = y + x = 0$. Navíc se jedná o grupu komutativní, protože sčítání reálných čísel je komutativní.

Pokud operaci grupy značíme symbolem „+“ (jako v tomto příkladě), pak obvykle o prvku e z vlastnosti (2) mluvíme jako o neutrálním prvku a značíme ho symbolem „0“ (též nula, nulový prvek) a prvek y z vlastnosti (3) nazývame *opačný* a značíme $-x$. Přičtení opačného prvku v komutativní grupě pak nazýváme *odečítání* a místo $a + (-b)$ píšeme $a - b$.

1.35. Příklad. Množina $\mathbf{R} \setminus \{0\}$ s operací násobení tvoří grupu. Skutečně platí asociativní zákon pro násobení reálných čísel: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, dále existuje jednotkový prvek 1, pro který $1 \cdot x = x \cdot 1 = 1$ a konečně pro každé $x \in \mathbf{R} \setminus \{0\}$ existuje $y = x^{-1}$ tak, že $x \cdot y = y \cdot x = 1$. Navíc se jedná o grupu komutativní, protože násobení reálných čísel je komutativní.

Pokud operaci grupy značíme symbolem „$\cdot$“, pak obvykle prvek e z vlastnosti (2) značíme symbolem „1“ (jedna, jednotkový prvek). Prvek y z vlastnosti (3) nazývame *inverzní* a značíme x^{-1}. Násobení inverzním prvkem v komutativní grupě nazýváme *dělení* a místo $a \cdot b^{-1}$ píšeme a/b nebo $\frac{a}{b}$.

1.36. Příklad. Množina $\mathbf{R}$ s operací násobení netvoří grupu, protože 0 nemá inverzní prvek.

1.37. Příklad. Množina všech reálných funkcí $F = \{f : \mathbf{R} \to \mathbf{R}$, f je prostá a „na“$\}$ s operací *skládání funkcí* $\circ : F \times F \to F$, definovanou pomocí $(g \circ f)(x) = g\big(f(x)\big)\ \forall x \in \mathbf{R}$, tvoří grupu. Skutečně platí asociativní zákon $(f \circ g) \circ h = f \circ (g \circ h)$ a existuje jednotkový prvek: identické zobrazení i, pro které $i(x) = x$. Ke každé prosté funkci f lze setrojit funkci inverzní f^{-1} tak, že $f \circ f^{-1} = f^{-1} \circ f = i$. Přitom se nejedná o grupu komutativní, protože například pro $f(x) = x^3$, $g(x) = 1 + x$ je $(f \circ g)(x) = (1 + x)^3$, zatímco $(g \circ f)(x) = 1 + x^3$.

1.38. Příklad. Kdybychom v předchozím příkladě místo funkcí f z $\mathbf{R}$ na $\mathbf{R}$ uvažovali prostá zobrazení p z nějaké množiny M na M, dostáváme znovu grupu, která nemusí být komutativní. V případě konečné množiny M se jedná o grupu permutací.

1.39. Příklad. S další grupou se seznámíme ve třetí kapitole. Množina všech regulárních matic stejného typu (n, n) (viz 3.51) s operací násobení matic tvoří příklad nekomutativní grupy.

1.40. Příklad. Množina čísel $\{0, 1, 2, \ldots, k-1\}$ s operací $a \oplus b = a + b$ modulo k tvoří komutativní grupu. Připomínáme, že „x modulo y" je zbytek při dělení čísla x číslem y. Neutrálním prvkem této grupy je 0 a opačným prvkem k prvku $a \neq 0$ je prvek $k - a$. Samozřejmě, opačným prvkem k prvku neutrálnímu je prvek neutrální, což ostatně platí v libovolné grupě.

1.41. Příklad. Lineární prostor se svou operací sčítání vektorů (podle definice 1.6) tvoří komutativní grupu. Skutečně, asociativní zákon je postulován vlastností (2) v definici 1.6, neutrálním prvkem je nulový vektor (viz vlastnost (1) věty 1.7) a opačný vektor k vektoru $\boldsymbol{x}$ je vektor $-\boldsymbol{x} = (-1) \cdot \boldsymbol{x}$, protože

$$(-1) \cdot \boldsymbol{x} + \boldsymbol{x} = (-1) \cdot \boldsymbol{x} + 1 \cdot \boldsymbol{x} = (-1 + 1) \cdot \boldsymbol{x} = 0 \cdot \boldsymbol{x} = \boldsymbol{o}.$$

Konečně z vlastnosti (1) definice 1.6 plyne, že se jedná o grupu komutativní.

1.42. Poznámka. Obráceně, pomocí pojmu grupa můžeme významně zkrátit naší definici lineárního prostoru 1.6:

Lineárním prostorem je množina L, která s operací $+ : L \times L \to L$ tvoří komutativní grupu. Dále musí být na množině L definována operace $\cdot : \mathbf{R} \times L \to L$, 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 1.6 přímo korespondují s vlastnostmi komutativní grupy, stačí ověřit, že nám z této nové definice vyplyne vlastnost (7) definice 1.6, která jediná zde chybí. Existence nulového vektoru je zajištěna jako existence neutrálního prvku $\boldsymbol{o}$ v grupě. Je potřeba ukázat, že pro libovolný $\boldsymbol{x} \in L$ je vektor $0 \cdot \boldsymbol{x}$ roven neutrálnímu prvku $\boldsymbol{o}$. K vektoru $0 \cdot \boldsymbol{x}$ ovšem existuje v grupě prvek opačný $-0 \cdot \boldsymbol{x}$. Ten přičteme k oběma stranám rovnice $0 \cdot \boldsymbol{x} = (0 + 0) \cdot \boldsymbol{x} = 0 \cdot \boldsymbol{x} + 0 \cdot \boldsymbol{x}$. Na levé straně dostáváme $0 \cdot \boldsymbol{x} + (-0 \cdot \boldsymbol{x}) = \boldsymbol{o}$. Na pravé straně je $0 \cdot \boldsymbol{x} + 0 \cdot \boldsymbol{x} + (-0 \cdot \boldsymbol{x}) = 0 \cdot \boldsymbol{x} + \boldsymbol{o} = 0 \cdot \boldsymbol{x}$. Porovnáním levé a pravé strany máme výsledek $\boldsymbol{o} = 0 \cdot \boldsymbol{x}$.

1.43. Poznámka. Axiomy grupy v definici 1.31 explicitně neuvádějí, že v grupě existuje jen jediný neutrální prvek a ke každému prvku existuje jen jediný prvek opačný. Následující věta ukazuje, že to nicméně platí jako jednoduchý důsledek axiomů.

1.44. Věta. (A) Každá grupa má jen jediný neutrální/jednotkový prvek. (B) Ke každému prvku grupy existuje jediný opačný/inverzní prvek.

Důkaz. (A) Předpokládáme dva neutrální prvky e_1, e_2. Musí platit $e_1 = e_1 \circ e_2$, protože e_2 je neutrální. Musí také platit $e_2 = e_1 \circ e_2$, protože e_1 je neutrální. Takže $e_1 = e_1 \circ e_2 = e_2$ a neutrální prvky se neliší.

(B) Nechť $x \in G$ má dva inverzní/opačné prvky y_1 a y_2. Označme e jednotkový prvek. Pak platí: $y_1 = e \circ y_1 = (y_2 \circ x) \circ y_1 = y_2 \circ (x \circ y_1) = y_2 \circ e = y_2$, takže $y_1 = y_2$.

1.45. Věta. Nechť na neprázdné množině G je dána operace $\circ : G \times G \to G$, pro kterou platí asociativní zákon (1) z definice grupy 1.31. Pak vlastnosti (2) a (3) z definice grupy jsou ekvivalentní s vlastností: pro každé $a, b \in G$ existují $x, y \in G$, které řeší rovnice $a \circ x = b$ a $y \circ a = b$.

Důkaz. Nechť nejprve platí vlastnosti (1), (2), (3) z definice grupy 1.31. Označme a^{-1} inverzní prvek k prvku a. Pak $x = a^{-1} \circ b$ řeší rovnici $a \circ x = b$, protože $a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b$. Z podobných důvodů $y = b \circ a^{-1}$ řeší rovnici $y \circ a = b$.

Nechť nyní platí asociativní zákon (1) a umíme řešit uvedené rovnice. Volme $a \in G$. Označme e_a řešení rovnice $a \circ x = a$, tj. platí $a \circ e_a = a$. Ukážeme nejprve, že pro libovolné $b \in G$ je $b \circ e_a = b$. Nechť $y \in G$ řeší rovnici $y \circ a = b$. Pak platí $b \circ e_a = (y \circ a) \circ e_a = y \circ (a \circ e_a) = y \circ a = b$. Vidíme tedy, že řešení e_a rovnice $a \circ x = a$ nezávisí na volbě prvku a, takže stačí prvek e_a označovat e. Podobně lze ukázat, že také řešení rovnice $y \circ a = a$ nezávisí na volbě prvku a. Označme toto řešení f. Nyní podobně jako v důkazu věty 1.44 je $f \circ e = f$, protože e řeší $a \circ e = a$ a platí $f \circ e = e$, protože f řeší $y \circ a = a$. Takže $e = f$ a toto je jednotkový prvek grupy.

Sestrojíme inverzní prvek k prvku $x \in G$. Nechť u řeší rovnici $x \circ u = e$ a v řeší rovnici $v \circ x = e$. Platí $v = v \circ e = v \circ (x \circ u) = (v \circ x) \circ u = e \circ u = u$, takže $u = v$ je inverzní prvek k prvku x.

1.46. Poznámka. Vzhledem k předchozí větě se v některé literatuře definuje grupa jen pomocí asociativního zákona a řešitelnosti rovnic (jen dvě vlastnosti). Pokud platí jen asociativní zákon a řešitelnost rovnic není požadována, mluví se o *pologrupě*. Pokud je pouze dána operace $\circ\colon G \times G \to G$ bez dalších vlastností, mluví se v některé literatuře o *grupoidu*. Takže množina s operací je grupoid. Grupoid s asociativním zákonem je pologrupa. Pologrupa s řešitelností rovnic je grupa. *Pologrupa, grupoid*

1.47. Definice. Nechť G je grupa s operací $\circ$. Pokud $G_1 \subset G$ je sama o sobě grupou se stejnou operací (tj. speciálně $\circ\colon G_1 \times G_1 \to G_1$ a platí vlastnosti (1)–(3) definice grupy 1.31), nazýváme G_1 *podgrupou* grupy G. *Podgrupa*

1.48. Poznámka. Výše uvedenou definici uvádím hlavně proto, aby měl čtenář možnost ji porovnat s definicí podprostoru 1.17 a shledal, že základní myšlenka definice podstruktury je pořád stejná. V případě ověřování podgrupy je kontrola asociativního zákona (1) zbytečná (je zaručen už ve vnější grupě), ale vlastnosti $x \circ y \in G_1$, $e \in G_1$ a existence inverzního prvku v G_1 jsou podstatné.

1.49. Příklad. Množina $\mathbf{Z}$ celých čísel s operací sčítání „+“ je podgrupou grupy $\mathbf{R}$ reálných čísel se stejnou operací.

1.50. Příklad. Množina $\mathbf{Z} \setminus \{0\}$ celých nenulových čísel s operací násobení „·“ není podgrupou grupy $\mathbf{R} \setminus \{0\}$ reálných čísel se stejnou operací, protože k číslům různým od -1 a 1 neexistuje na množině $\mathbf{Z} \setminus \{0\}$ inverzní prvek. Na druhé straně se jedná o pologrupu, protože násobení je uzavřeno na nenulová celá čísla a je samozřejmě asociativní.

1.51. Definice. *Těleso* je množina T se dvěma operacemi obvykle označovanými $+\colon T \times T \to T$ a $\cdot\colon T \times T \to T$, které mají následující vlastnosti: *Těleso*

(1) T s operací „+“ je komutativní grupa. Neutrální prvek této grupy je označen symbolem 0.
(2) $T \setminus \{0\}$ s operací „·“ je komutativní grupa. Jednotkový prvek této grupy se značí symbolem 1.
(3) Operace „+“ a „·“ splňují distributivní zákon: $a \cdot (b + c) = a \cdot b + a \cdot c$.

1.52. Poznámka. Někteří autoři v definici tělesa nepožadují komutativitu grupy vzhledem k násobení a pokud je splněna, mluví o *komutativním tělese*. Existují příklady, kdy komutativita násobení není splněna Důležitým příkladem jsou *kvaterniony*: čísla podobná komplexním, ale se třemi nezávislými imaginárními jednotkami. Kvaterniony se užívají například při popisu 3D transformací v počítačové grafice [26]. V našem textu budeme u těles vždy předpokládat komutativitu obou operací.

1.53. Příklad. Reálná čísla s operacemi sčítání a násobení tvoří těleso.

1.54. Příklad. Racionální čísla jsou podtělesem tělesa reálných čísel. Podtěleso je definováno v souladu s poznámkou 1.48 jako podmnožina tělesa, která sama o sobě se stejnými operacemi tvoří těleso.

1.55. Příklad. Množina celých čísel s operacemi sčítání a násobení netvoří těleso, protože pro operaci násobení neexistuje pro všechna nenulová celá čísla inverzní prvek jako celé číslo. Toto je příklad struktury, která má všechny vlastnosti tělesa s výjimkou jediné: není zaručena existence inverzního prvku pro násobení. Taková struktura se nazývá *okruh*.

1.56. Příklad. Množina komplexních čísel s operacemi sčítání a násobení tvoří těleso.

1.57. Věta. Pro libovolné prvky a, b z tělesa platí: $a \cdot b = 0$ právě tehdy, když $a = 0$ nebo $b = 0$.

Důkaz. ($\Rightarrow$): $T \setminus \{0\}$ musí být podle vlastnosti (2) definice 1.51 vzhledem k násobení grupa, tj. součin dvou nenulových prvků musí být prvek nenulový. Jinými slovy, pokud součin vychází nulový, musí aspoň jeden z činitelů být nula.

($\Leftarrow$): Je třeba dokázat, že $0 \cdot a = 0$. Protože 0 je neutrální prvek vzhledem ke sčítání, platí $0 + 0 = 0$. Díky distributivnímu zákonu je $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$. K oběma stranám rovnosti přičteme opačný prvek k prvku $0 \cdot a$, tedy prvek $-0 \cdot a$. Na levé straně dostáváme 0 a na pravé $0 \cdot a$.

1.58. Příklad. Těleso musí podle definice obsahovat 0 a 1 a tyto dva prvky musejí být různé. Takže těleso musí obsahovat aspoň dva prvky. Ukážeme, že existuje těleso, které obsahuje jen tyto dva prvky, tedy $T = \{0, 1\}$. *Galoisovo těleso se dvěma prvky*

Operaci „+“ definujeme: $0+0=0,\ 0+1=1+0=1,\ 1+1=0$. Operaci „·“ definujeme jako obvyklé násobení: $0\cdot 0=0\cdot 1=1\cdot 0=0,\ 1\cdot 1=1$. Množina $T=\{0,1\}$ s takto zavedenými operacemi tvoří těleso.

Skutečně, pro operaci „+“ platí asociativní zákon, 0 je neutrální prvek, opačný prvek k 0 je 0 a opačný prvek k 1 je 1. Grupa $T\setminus\{0\}$ vzhledem k násobení je jednoprvková a všechny vlastnosti grupy zde platí zcela samozřejmě. Je rovněž splněn distributivní zákon.

Sčítání je v tomto tělese totéž co odečítání. Inverzní prvek k 1 je 1.

Tělesa s konečně mnoha prvky se z historických důvodů nazývají *Galoisova tělesa.* V našem příkladě $T=\{0,1\}$ se tedy jedná o Galoisovo těleso se dvěma prvky.

Évariste Galois byl francouzský matematik, který bohužel zemřel mlád ve věku 20 let na následky zranění v souboji. I jeho teorie dokazuje mimo jiné nemožnost algebraického popisu kořenů polynomů stupně většího než 4. Tato teorie je známější než Abelova, ovšem byla zveřejněna o pět let později.

1.59. Poznámka. Chceme-li na dvouprvkové množině definovat operace sčítání a násobení tak, abychom získali těleso, nemůžeme to udělat jinak, než v příkladu 1.58. Především 0 je neutrální prvek vzhledem ke sčítání, takže podle vlastnosti (2) definice grupy 1.31 musí $0+0=0$, $0+1=1+0=1$. Dále množina $\{1\}$ musí být grupou vzhledem k násobení, takže musí $1\cdot 1=1$. Dále musí platit $0\cdot a=a\cdot 0=0$, jinak by nebyla splněna věta 1.57. Zbývá otázka, zda můžeme definovat $1+1=1$. Nemůžeme, protože pak by prvek 1 neměl prvek opačný.

1.60. Příklad. Na množině $\{0,1,\dots,p-1\}$ definujme operace „+“ a „·“ jako obvyklé sčítání a násobení, ovšem na výsledek aplikujme proces „modulo p“. Takže například pro $p=5$ pracujeme s množinou $\{0,1,2,3,4\}$ a platí $4+3=2$, protože zbytek po dělení čísla 7 číslem 5 je 2. Nebo $4\cdot 4=1$, protože zbytek po dělení čísla 16 číslem 5 je 1. GF(p), $\mathbf{Z}_p$

Nechť nejprve p není prvočíslo, tj. je tvaru součinu $p=m\,n$. Pak $m\cdot n=0$ modulo p, a přitom čísla m a n jsou nenulová. Podle věty 1.57 se nemůže jednat o těleso, protože součin nenulových čísel musí v tělese vyjít jako číslo nenulové.

Nechť p je prvočíslo. Ukážeme, že $M=\{0,1,\dots,p-1\}$ s operacemi „+, · modulo p“ tvoří těleso. Především M se sčítáním modulo p je komutativní grupa (viz příklad 1.40). Operace násobení modulo p je asociativní, komutativní a jednotkovým prvkem je číslo 1. Distributivní zákon plyne z distributivního zákona běžných operací „+“ a „·“. Nejvíce práce dá nalezení inverzního prvku pro $a\in M\setminus\{0\}$. Prvek a nechme pevný a uvažujme všechna čísla „ak modulo p“ pro $k\in\{1,2,\dots,p-1\}$. Tato čísla jsou pro různá k vzájemně různá (viz níže) a pokrývají tedy celou množinu $\{1,2,\dots,p-1\}$. Musí tedy existovat takové k, že $ak=1 \bmod p$. Toto k je inverzním prvkem k prvku a. V úvaze ještě chybí obhájit, že čísla „ak modulo p“ jsou pro různá k vzájemně různá. Předpokládejme, že existují čísla $k_1,k_2\in M\setminus\{0\}$, $k_1\ge k_2$ taková, že $ak_1=ak_2 \bmod p$, tj. $a(k_1-k_2)=mp$ pro nějaké $m\ge 0$. Rovnost vydělíme číslem a. Protože $a<p$ a p je prvočíslo, existuje $m_1\ge 0$, že po vydělení číslem a dostáváme $k_1-k_2=m_1p$. Vlevo je číslo menší než p, takže musí být $m_1=0$, tj. $k_1=k_2$.

Podle počtu prvků p se toto těleso označuje GF(p). Jiné značení $\mathbf{Z}_p$ dává najevo, že se jedná o celá čísla „modulo p“. Předchozí příklad 1.58 definuje konečné těleso $\mathbf{Z}_p$ pro $p=2$.

1.61. Definice. *Charakteristika tělesa* udává nejmenší kladný počet jedniček, jejichž součet dává nulu. Tedy pokud je $\sum_1^\lambda 1=0$ a λ je nejmenší kladné číslo s touto vlastností, pak těleso má charakteristiku λ. Pokud tato vlastnost není splněna pro žádný počet jedniček, je charakteristika rovna ∞.

1.62. Příklad. Charakteristika tělesa reálných čísel je ∞. Charakteristika tělesa $\mathbf{Z}_p$ je p.

1.63. Věta. Charakteristika tělesa je nekonečná nebo to je prvočíslo.

Důkaz. Sporem. Nechť pro charakteristiku λ platí $\lambda=mn$, $m\ne\lambda$, $n\ne\lambda$. Z distributivního zákona plyne $(\sum_1^m 1)\cdot(\sum_1^n 1)=\sum_1^{mn}1=\sum_1^\lambda 1=0$. Podle věty 1.57 musí být aspoň jedna suma v závorce rovna nule, protože jejich součin je nulový. To je spor s tím, že λ je nejmenší počet jedniček, jejichž součet je nulový.

1.64. Poznámka. Kromě GF(p), kde p je prvočíslo, existují konečná tělesa s počtem prvků p^m, kde p je prvočíslo, m je libovolná mocnina, značení: GF(p^m). Jak jsme ukázali v příkladě 1.60, konstrukce operací pro GF(p^m) nemůže vycházet jen z myšlenky „modulo p“. Ve skutečnosti je konstrukce tělesa GF(p^m) výrazně komplikovanější. V následujícím příkladě je pro ilustraci popsáno těleso GF(2^3).

Z věty 1.63 plyne, že i tělesa $\mathrm{GF}(p^m)$ musejí mít charakteristiku ve tvaru prvočísla. Kdybychom zde měli prostor na podrobnější popis těles $\mathrm{GF}(p^m)$, shledali bychom, že mají charakteristiku p.

Dá se dále ukázat, že pokud má mít těleso konečný počet prvků, pak tento počet nemůže být jiný než p^m, kde p je prvočíslo a m přirozené číslo. Navíc operace na konečném tělese lze definovat jediným možným způsobem (lišit se může jen způsob označení prvků).

1.65. Příklad. Uvažujme množinu všech uspořádaných trojic prvků ze $\mathbf{Z}_2$ indexovaných čísly. Nulová trojice nemá žádný index a ostatní trojice mají přiřazeny indexy 0 až 6:

$$\{(0,0,0)_*,\ (1,0,0)_0,\ (0,1,0)_1,\ (0,0,1)_2,\ (1,1,0)_3,\ (0,1,1)_4,\ (1,1,1)_5,\ (1,0,1)_6\}.$$

Prvky této množiny budeme sčítat tak, že si indexů nebudeme všímat a budeme sčítat jen uspořádané trojice v aritmetice $\mathbf{Z}_2$. Například $(1,1,0)_3 + (0,1,1)_4 = (1,0,1)_6$, protože je $(1,1,0)+(0,1,1) = (1,0,1)$ v aritmetice $\mathbf{Z}_2$.

Výsledek násobení kteréhokoli prvku s prvkem $(0,0,0)_*$ definujeme jako $(0,0,0)_*$. Jedná se o nulový prvek tělesa. Násobení nenulových prvků definujeme tak, že si nevšímáme uspořádaných trojic, ale jen indexů. Ty sečteme a provedeme operaci modulo 7. Například $(0,1,1)_4 \cdot (1,1,1)_5 = (0,0,1)_2$, protože $4+5$ modulo $7 = 2$. Dá se ukázat, že tento příklad splňuje axiomy tělesa. Obsahuje 2^3 prvků, takže se jedná o příklad tělesa $\mathrm{GF}(2^3)$.

Jak již bylo řečeno, je $(0,0,0)_*$ nulový prvek. Rovněž je zřejmé, že $(1,0,0)_0$ je jednotkový prvek tohoto tělesa. Inverzní prvek například k $(0,0,1)_2$ je $(1,1,1)_5$, protože $2+5$ modulo $7 = 0$. Opačný prvek k libovolnému prvku x je prvek x, protože v aritmetice $\mathbf{Z}_2$ je $1+1=0$. Charakteristika tohoto tělesa je 2.

Prosím čtenáře, aby se nesnažil hrubou silou ověřit platnost distributivního zákona tohoto tělesa (jde to, ale není to příliš účelné) ani příliš nehloubal nad tím, proč například trojice $(1,1,1)$ má index 5. Pro odpovědi na tyto otázky je potřeba použít vlastnosti ireducibilních polynomů nad tělesem $\mathbf{Z}_2$ (obecně nad tělesem $\mathbf{Z}_p$), což bohužel překračuje rámec tohoto úvodního textu.

1.66. Poznámka. V definici lineárního prostoru 1.6 jsme sice byli dostatečně abstraktní (vektory, ani operace s nimi jsme blíže nespecifikovali), ale pracovali jsme tam s docela konkrétní množinou $\mathbf{R}$ reálných čísel. Pokud v této definici nahradíme množinu $\mathbf{R}$ pojmem těleso (s blíže nespecifikovanými prvky a operacemi), dostáváme lineární prostor nad tělesem. Můžeme pak pracovat s lineárním prostorem nad tělesem komplexních čísel, lineárním prostorem nad tělesem $\mathbf{Z}_2$ atd. *Lineární prostor nad tělesem*

Pokusíme se tedy do třetice přepsat definici lineárního prostoru, tentokrát nad libovolným tělesem.

1.67. Definice. Množinu L nazýváme *lineárním prostorem nad tělesem* T, pokud jsou definovány operace $+\colon L\times L \to L$ a $\cdot\colon T\times L\to L$ tak, že L tvoří s operací $+$ komutativní grupu, a dále $\forall\alpha,\beta\in T, \forall\boldsymbol{x},\boldsymbol{y}\in L$:

$$\begin{aligned}
&\text{(A)}\quad \alpha\cdot(\beta\cdot\boldsymbol{x}) = (\alpha\cdot\beta)\cdot\boldsymbol{x},\\
&\text{(B)}\quad \alpha\cdot(\boldsymbol{x}+\boldsymbol{y}) = \alpha\cdot\boldsymbol{x}+\alpha\cdot\boldsymbol{y},\\
&\text{(C)}\quad (\alpha+\beta)\cdot\boldsymbol{x} = \alpha\cdot\boldsymbol{x}+\beta\cdot\boldsymbol{x},\\
&\text{(D)}\quad 1\cdot\boldsymbol{x} = \boldsymbol{x}.
\end{aligned}$$

1.68. Poznámka. Volíme-li za těleso T v této definici množinu reálných čísel $\mathbf{R}$, dostáváme vzhledem k poznámce 1.42 definici lineárního prostoru 1.6. Abych uklidnil čtenáře, tak konstatuji, že v dalších kapitolách tohoto textu nebudeme potřebovat lineární prostor v takové obecnosti (nad libovolným tělesem) a vystačíme si většinou s lineárním prostorem nad reálnými čísly. Pokud tedy nebude výslovně řečeno jinak (například lineární prostor nad $\mathbf{Z}_2$ studovaný v kapitole 10), pak pojmem *lineární prostor* myslíme lineární prostor nad $\mathbf{R}$ a stačí použít definici 1.6.

1.69. Příklad. Vrátíme se k příkladu lineárního prostoru reálných uspořádaných n-tic 1.11 a zobecníme ho na lineární prostor uspořádaných n-tic prvků libovolného tělesa.

Nechť T je těleso. Uvažujme množinu uspořádaných n-tic prvků z tělesa T (označme ji T^n) a definujme na ni operace $+\colon T^n\times T^n\to T^n$, $\cdot\colon T\times T^n\to T^n$ takto: pro každé $(a_1,\ldots,a_n)\in T^n$, $(b_1,\ldots,b_n)\in T^n$, $\alpha\in T$ je

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

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

Snadno se dá ověřit, že množina T^n s takto definovanými operacemi tvoří lineární prostor nad tělesem T.

1.70. Poznámka. Volíme-li za těleso $T = \mathbf{Z}_2$, je T^n podle předchozího příkladu diskrétní lineární prostor, který je používán v teorii kódování. Jednotlivé vektory (tzv. binární slova) jsou uspořádané n-tice jedniček a nul. Tento lineární prostor má celkem 2^n různých vektorů.

1.71. Poznámka. V případě lineárního prostoru nad konečným tělesem dostáváme konečný lineární prostor. V tomto případě tedy neplatí tvrzení poznámky 1.27. Můžete si všimnout, že toto tvrzení se opíralo o skutečnost, že „reálných čísel je nekonečně mnoho“. Poznámka 1.27 zůstává v platnosti pro lineární prostory nad nekonečnými tělesy.

2. Lineární závislost a nezávislost, lineární obal, báze, dimenze

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

Tyto vlastnosti a pojmy předpokládají pouze to, že vektory (tj. prvky nějaké blíže neurčené množiny) umíme sčítat a násobit reálným číslem, a přitom tyto operace splňují vlastnosti (1) až (7) z definice 1.6. Kdybychom tuto jednotící definici neměli, museli bychom například zvlášť zavádět pojmy lineární závislost, báze a dimenze pro množinu orientovaných úseček, zvlášť pro množinu uspořádaných n-tic a zvlášť pro množinu reálných funkcí. Až bychom třeba později zjistili, že můžeme kupříkladu nekonečné posloupnosti reálných čísel sčítat a násobit skalárem, znovu bychom pro tuto množinu byli nuceni definovat pojmy lineární závislost, báze a dimenze. Přitom k zavedení těchto pojmů je zapotřebí dokázat několik tvrzení, která bychom tak museli dokazovat pro každou konkrétní množinu zvlášť. Snad každý uzná, že to je docela zbytečná práce. Je přeci jen jednodušší ověřit, že nějaká množina tvoří lineární prostor a okamžitě pro ni používat všechny další vlastnosti a pojmy, které se dozvíme v této kapitole.

2.2. Poznámka. Sčítání má podle definice 1.6 dva operandy. Když bychom chtěli sečíst třeba tři vektory $\boldsymbol{x}+\boldsymbol{y}+\boldsymbol{z}$, měli bychom uvést, v jakém pořadí budeme operace provádět, tj. zda provedeme $(\boldsymbol{x}+\boldsymbol{y})+\boldsymbol{z}$ nebo $\boldsymbol{x}+(\boldsymbol{y}+\boldsymbol{z})$. Vlastnost (2) definice 1.6 nás ale od této povinnosti osvobozuje, protože zaručuje, že oba případy povedou ke stejnému výsledku. Proto nebudeme v takovém případě nadále závorky uvádět a například pro vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ budeme jejich součet zapisovat jednoduše: $\boldsymbol{x}_1+\boldsymbol{x}_2+\cdots+\boldsymbol{x}_n$.

Dále budeme místo $\boldsymbol{x}+(-1)\cdot\boldsymbol{y}$ zapisovat stručně $\boldsymbol{x}-\boldsymbol{y}$. Tím vlastně máme zavedenu operaci odčítání vektorů, ačkoli tato operace není v definici 1.6 vůbec zmíněna.

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

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

Lineární kombinace

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

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

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

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

Triviální lineární kombinace

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

Důkaz. Podle vlastnosti (7) v definici 1.6 je každý sčítanec v triviální lineární kombinaci roven nulovému vektoru a podle vlastnosti (1) věty 1.7 je i součet nulových vektorů roven nulovému vektoru.

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

Lineární závislost skupiny

2.8. Poznámka. Pokud bychom rozvedli pojem netriviální lineární kombinace podle definic 2.5 a 2.3, můžeme říci, že vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou *lineárně závislé*, pokud existují reálná čísla $\alpha_1, \alpha_2, \ldots, \alpha_n$ tak, že aspoň jedno z nich je nenulové, a přitom platí

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

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

Lineární nezávislost skupiny

2.10. Poznámka. Vektory jsou lineárně nezávislé, pokud (podle definic 2.7 a 2.9) neexistuje netriviální lineární kombinace těchto vektorů, která je rovna nulovému vektoru. Jinak řečeno, jedině triviální lineární kombinace je rovna nulovému vektoru. Při použití definice 2.5 můžeme říci, že vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou lineárně nezávislé, pokud z předpokladu $\alpha_1 \cdot \boldsymbol{x}_1 + \alpha_2 \cdot \boldsymbol{x}_2 + \cdots + \alpha_n \cdot \boldsymbol{x}_n = \boldsymbol{o}$ nutně plyne, že $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

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

Pojem lineární závislosti a nezávislosti vektorů má v lineární algebře zásadní důležitost. Závislost vektorů je možná názornější z pohledu následující věty 2.21, ovšem při ověřování lineární závislosti abstraktních vektorů je definice 2.7 použitelnější. Má proto smysl definicím 2.7 a 2.9 věnovat náležitou pozornost.

2.12. Příklad. Uvažujme lineární prostor $\mathbf{R}^3$ (viz příklad 1.11, $n = 3$). Jsou dány tři vektory z $\mathbf{R}^3$:

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

Zjistíme z definice, zda jsou vektory $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ lineárně závislé či nezávislé. Podle poznámek 2.8 a 2.10 stačí zjistit, jaké mohou být koeficienty α, β, γ, pokud položíme

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

Dosazením do této rovnice dostáváme

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

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

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

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

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

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

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

Existuje tedy netriviální lineární kombinace vektorů $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$, která je rovna nulovému vektoru, což podle definice 2.7 znamená, že vektory $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ jsou lineárně závislé.

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

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

Zjistíme z definice, zda jsou vektory $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ lineárně závislé či nezávislé. Podle poznámek 2.8 a 2.10 stačí zjistit, jaké mohou být koeficienty α, β, γ, pokud položíme $\alpha\, \boldsymbol{x} + \beta\, \boldsymbol{y} + \gamma\, \boldsymbol{z} = \boldsymbol{o}$. Dosazením do této rovnice dostáváme

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

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

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

Tato soustava má jediné řešení $\alpha = 0$, $\beta = 0$, $\gamma = 0$ (zkuste si to ověřit třeba Gaussovou eliminační metodou). Vidíme tedy, že jedině triviální lineární kombinace vektorů $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ je rovna nulovému vektoru, což podle definice 2.9 znamená, že vektory $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ jsou lineárně nezávislé.

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

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

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

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

a zjistíme, jakých hodnot mohou nabývat koeficienty α, β, γ. Tato rovnost má být splněna pro všechna $x \in \mathbf{R}$. Je možné, že při volbě tří hodnot $x \in \mathbf{R}$ už vynutíme trivialitu lineární kombinace v (2.1). Zkusme štěstí například pro $x \in \{0, \frac{\pi}{2}, \pi\}$. V rovnici (2.1) se tedy omezíme na

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

Po dosazení hodnot x dostáváme tři rovnice:

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

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

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

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

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

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

a zjistíme, jakých hodnot mohou nabývat koeficienty α, β, γ. Jako v příkladu 2.14 zkusíme volit nějaké tři hodnoty x. Po dosazení $x = 0$, $x = \pi/2$ a $x = \pi$ dostáváme soustavu

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

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

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

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

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

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

lineárně závislé.

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

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

Dosadíme:

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

a po úpravách dostáváme

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

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

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

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

Základní vlastnosti lineární (ne)závislosti

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

Důkaz. (1) Lineární kombinace vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ nezávisí na jejich pořadí, protože sčítání vektorů je podle definice 1.6 komutativní.

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

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

což je netriviální lineární kombinace rovna nulovému vektoru.

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

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

což je netriviální lineární kombinace rovna nulovému vektoru.

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

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

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

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

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

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

Kdyby bylo $\alpha \neq 0$, mohli bychom psát

$$\boldsymbol{x}_1 = 1 \cdot \boldsymbol{x}_1 = \left(\frac{1}{\alpha}\,\alpha\right) \cdot \boldsymbol{x}_1 = \frac{1}{\alpha}\,(\alpha\,\boldsymbol{x}_1) = \frac{1}{\alpha} \cdot \boldsymbol{o} = \boldsymbol{o}.$$

To je ale spor. Musí tedy být $\alpha = 0$. To znamená, že pouze triviální lineární kombinace je rovna nulovému vektoru, takže vektor $\boldsymbol{x}_1$ je lineárně nezávislý.

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

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

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

Podle definice lineární závislosti hledejme netriviální lineární kombinaci, pro kterou

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

Rozepsáním tohoto požadavku do složek dostáváme n rovnic o m neznámých. Protože pravé strany rovnic jsou nulové, soustava má určitě aspoň triviální řešení. Protože je v soustavě více neznámých než rovnic existuje nekonečně mnoho řešení této soustavy. Mezi těmito řešeními je jen jediné triviální a všechna ostatní jsou netriviální. Poznamenejme ještě, že matematicky korektnější argumentace k tomuto příkladu vychází jako důsledek věty 2.56.

Poznamenejme, že příklad ukazuje důležitou vlastnost lineárních prostorů $\mathbf{R}^n$: všechny lineárně nezávislé skupiny vektorů mají počet vektorů menší nebo roven n.

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

Jeden vektor je lineární kombinací ostatních

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

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

$$\alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_n \boldsymbol{x}_n = \sum_{i=1}^{n} \alpha_i \boldsymbol{x}_i = \boldsymbol{o}, \tag{2.3}$$

a přitom aspoň jeden koeficient lineární kombinace je nenulový. Existuje tedy $r \in \{1, \ldots, n\}$ takové, že $\alpha_r \neq 0$. Přičteme nyní vektor $-\alpha_r \boldsymbol{x}_r$ k oběma stranám rovnice (2.3)

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

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

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

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

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

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

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

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

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

2.22. Poznámka. Věta 2.21 se dá přeformulovat též takto: vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou lineárně nezávislé právě tehdy, když žádný z vektorů $\boldsymbol{x}_i$, $i \in \{1, \ldots, n\}$, není lineární kombinací ostatních vektorů.

2.23. Poznámka. Věta 2.21 má pro $n = 2$ tento důsledek: dva nenulové vektory $\boldsymbol{x}, \boldsymbol{y}$ jsou lineárně závislé právě tehdy, když existuje $\alpha \in \mathbf{R}$ tak, že $\boldsymbol{x} = \alpha\, \boldsymbol{y}$. Lidově řečeno: jeden vektor je násobkem druhého.

2.24. Příklad. Uvažujme lineární prostor U_O všech orientovaných úseček z příkladu 1.24.

Závislost orientovaných úseček

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

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

Abychom to dokázali, potřebujeme určitou představivost a zkušenosti s euklidovskou geometrií. Připomeňme, že O značí společný počátek všech orientovaných úseček našeho lineárního prostoru. Zvolme nyní libovolnou orientovanou úsečku $\boldsymbol{x}$ s počátkem v O, která leží v rovině určené úsečkami $\boldsymbol{u}, \boldsymbol{v}$. Ukážeme, že existují $\alpha, \beta \in \mathbf{R}$ tak, že $\boldsymbol{x} = \alpha\, \boldsymbol{u} + \beta\, \boldsymbol{v}$. Leží-li $\boldsymbol{x}$ na společné přímce s úsečkou $\boldsymbol{u}$ nebo na přímce společné s úsečkou $\boldsymbol{v}$, pak je $\boldsymbol{x}$ násobkem této úsečky a druhý koeficient hledané lineární kombinace je nulový. Nechť tedy $\boldsymbol{x}$ neleží na žádné z těchto přímek. Koncový bod úsečky $\boldsymbol{x}$ označme X. Veďme bodem X rovnoběžku s úsečkou $\boldsymbol{u}$ a rovnoběžku s úsečkou $\boldsymbol{v}$. První z nich nutně protne přímku, na které leží úsečka $\boldsymbol{v}$, v nějakém bodě P a druhá protne přímku, na které leží úsečka $\boldsymbol{u}$, v nějakém bodě Q. Zvolme $\alpha, \beta \in \mathbf{R}$ tak, aby $\alpha\, \boldsymbol{u} = \overrightarrow{OQ}$ a $\beta\, \boldsymbol{v} = \overrightarrow{OP}$ (symbolem $\overrightarrow{OA}$ značíme orientovanou úsečku s počátkem v bodě O a koncem v bodě A). Z definice sčítání orientovaných úseček pomocí rovnoběžníka vidíme, že $\boldsymbol{x} = \alpha\, \boldsymbol{u} + \beta\, \boldsymbol{v}$. Udělejte si náčrtek.

(3) Leží-li tři usečky $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in U_O$ ve společné rovině, pak jsou lineárně závislé, protože z (2) plyne, že jedna z nich je lineární kombinací ostatních. Dále použijeme větu 2.21.

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

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

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

vyplňuje celý lineární prostor U_O.

Abychom to dokázali, potřebujeme opět určitou představivost. Nechť ϱ je rovina určená úsečkami $\boldsymbol{u}$ a $\boldsymbol{v}$. Ukážeme, že pro libovolnou orientovanou úsečku $\boldsymbol{x}$ s počátkem v O existují reálná čísla α, β, γ taková, že $\boldsymbol{x} = \alpha\, \boldsymbol{u} + \beta\, \boldsymbol{v} + \gamma\, \boldsymbol{w}$. Leží-li $\boldsymbol{x}$ v rovině ϱ, položíme $\gamma = 0$ a dále využijeme výsledku z (2). Nechť tedy $\boldsymbol{x}$ neleží v rovině ϱ. Označme X koncový bod úsečky $\boldsymbol{x}$. Veďme bodem X rovnoběžku s úsečkou $\boldsymbol{w}$. Ta nutně protne rovinu ϱ v nějakém bodě P. Podle (2) existují $\alpha, \beta \in \mathbf{R}$ takové, že $\overrightarrow{OP} = \alpha\, \boldsymbol{u} + \beta\, \boldsymbol{v}$. Nechť c je vzdálenost bodu X od bodu P. Pokud mezi bodem X a koncovým bodem úsečky $\boldsymbol{w}$ leží rovina ϱ, volme $\gamma = -c$, jinak volme $\gamma = c$. Z definice sčítání orientovaných úseček pomocí rovnoběžníka je vidět, že $\boldsymbol{x} = \overrightarrow{OP} + \gamma\, \boldsymbol{w} = \alpha\, \boldsymbol{u} + \beta\, \boldsymbol{v} + \gamma\, \boldsymbol{w}$.

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

2.26. Definice. Nechť L je lineární prostor. Neprázdná konečná množina vektorů $K \subseteq L$, $K = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$ se nazývá *lineárně závislá*, pokud jsou vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ lineárně závislé.

Lineární (ne)závislost nekonečných množin

Nekonečná množina vektorů $M \subseteq L$ se nazývá *lineárně závislá*, pokud existuje konečná $K \subseteq M$, která je lineárně závislá.

Množina $M \subseteq L$ se nazývá *lineárně nezávislá*, pokud není lineárně závislá.

Prázdnou množinu považujeme vždy za lineárně nezávislou.

2.27. Poznámka. Uvedeme si podrobněji, jak poznáme lineární nezávislost množin.

Neprázdná konečná množina vektorů $K \subseteq L$, $K = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$ se nazývá lineárně nezávislá, pokud jsou vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ lineárně nezávislé.

Nekonečná množina vektorů $M \subseteq L$ se nazývá lineárně nezávislá, pokud všechny konečné podmnožiny $K \subseteq M$ jsou lineárně nezávislé.

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

Podle definice 2.26 a poznámky za ní stačí ukázat, že každá konečná podmnožina polynomů

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

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

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

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

2.29. Definice. Nechť L je lineární prostor. *Lineární obal* skupiny vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ je množina všech lineárních kombinací vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$. *Lineární obal*

Lineární obal konečné množiny $K \subseteq L$, $K = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$ ztotožňujeme s lineárním obalem skupiny vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$.

Lineární obal nekonečné množiny $M \subseteq L$ je sjednocení lineárních obalů všech konečných podmnožin množiny M.

Lineární obal skupiny vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ značíme $\langle \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \rangle$. Lineární obal množiny M značíme symbolem $\langle M \rangle$.

2.30. Poznámka. Jsou-li $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ vektory nějakého lineárního prostoru L, pak podle definice 2.29 je

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

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

Podle poznámky 2.30 je

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

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

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

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

Po úpravě a porovnání jednotlivých složek dostáváme soustavu

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

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

2.33. Poznámka. Zamysleme se nad tím, co to znamená, že $\boldsymbol{z} \in \langle M \rangle$. Existuje konečná podmnožina $K \subseteq M$ taková, že $\boldsymbol{z} \in \langle K \rangle$. Nechť $K = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$. Skutečnost, že $\boldsymbol{z} \in \langle K \rangle$ znamená, že existuje nějaká lineární kombinace vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$, která je rovna vektoru $\boldsymbol{z}$. *Prvek lineárního obalu*

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

$$\boldsymbol{z} = \alpha_1\, \boldsymbol{x}_1 + \alpha_2\, \boldsymbol{x}_2 + \cdots + \alpha_n\, \boldsymbol{x}_n. \tag{2.4}$$

2.34. Věta. Nechť L je lineární prostor, $M \subseteq L$, $N \subseteq L$. Pokud je $M \subseteq N$, pak platí $\langle M \rangle \subseteq \langle N \rangle$.

Vlastnosti lineárního obalu

Důkaz. Nechť $\boldsymbol{z} \in \langle M \rangle$, tj. předpokládáme, že $\boldsymbol{z}$ lze zapsat jako lineární kombinaci konečně mnoha prvků z M. Protože tyto prvky leží i v N, můžeme říci, že $\boldsymbol{z}$ lze zapsat jako lineární kombinaci konečně mnoha prvků z N. To podle poznámky 2.33 znamená, že $\boldsymbol{z} \in \langle N \rangle$.

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

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

Důkaz. (1) Stačí ukázat, že pokud $\boldsymbol{z} \in M$ pak $\boldsymbol{z} \in \langle M \rangle$. Platí $\boldsymbol{z} = 1 \cdot \boldsymbol{z}$, takže pro $\boldsymbol{z}$ existuje konečně mnoho prvků z M (jmenovitě prvek $\boldsymbol{z}$ samotný) tak, že $\boldsymbol{z}$ je lineární kombinací těchto prvků. To podle poznámky 2.33 znamená, že $\boldsymbol{z} \in \langle M \rangle$.

(2) Protože platí věta 2.34 a vzhledem k (1) stačí ukázat, že $\langle \langle M \rangle \rangle \subseteq \langle M \rangle$. Nechť $\boldsymbol{z} \in \langle \langle M \rangle \rangle$, ukážeme že $\boldsymbol{z} \in \langle M \rangle$. Protože $\boldsymbol{z} \in \langle \langle M \rangle \rangle$, existují vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \in \langle M \rangle$ takové, že platí (2.4). Pro každé $i \in \{1, \ldots, n\}$ je $\boldsymbol{x}_i \in \langle M \rangle$, tj. existuje konečně mnoho vektorů $\boldsymbol{y}_{i,1}, \ldots, \boldsymbol{y}_{i,k_i} \in M$ takových, že

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

Dosazením těchto rovnic do (2.4) a roznásobením dostáváme výsledek, že $\boldsymbol{z}$ je lineární kombinací konečně mnoha vektorů $\boldsymbol{y}_{i,j} \in M$, $i \in \{1, \ldots, n\}, j \in \{1, \ldots, k_i\}$. To znamená, že $\boldsymbol{z} \in \langle M \rangle$.

(3) Toto tvrzení je důsledkem (1) a (2). Protože $M \subseteq \langle M \rangle$ a $\{\boldsymbol{z}\} \subseteq \langle M \rangle$, je $M \cup \{\boldsymbol{z}\} \subseteq \langle M \rangle$. Obalením levé i pravé strany této množinové inkluze dostáváme $\langle M \cup \{\boldsymbol{z}\} \rangle \subseteq \langle \langle M \rangle \rangle = \langle M \rangle$. Obrácená inkluze plyne z věty 2.34.

2.36. Poznámka. Vlastnost (1) věty 2.35 lidově řečeno znamená, že „lineární obalení" množiny může přidat do této množiny další prvky, ale pokud tento proces zopakujeme, další prvky už podle vlastnosti (2) nezískáme.

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

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

Lineární obal je podprostor

Důkaz. Dokážeme nejprve „M je lineární podprostor, potom $\langle M \rangle = M$". Vezmeme $\boldsymbol{z} \in \langle M \rangle$ a dokážeme, že $\boldsymbol{z} \in M$. Protože $\boldsymbol{z} \in \langle M \rangle$, existuje konečně mnoho vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \in M$ takových, že lze psát $\boldsymbol{z} = \alpha_1\, \boldsymbol{x}_1 + \alpha_2\, \boldsymbol{x}_2 + \cdots + \alpha_n\, \boldsymbol{x}_n$. Každý sčítanec leží podle vlastnosti (2) definice 1.17 v množině M. Podle vlastnosti (1) definice 1.17 v množině M leží i součet těchto vektorů, tedy $\boldsymbol{z} \in M$.

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

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

Důkaz. Skutečnost, že $P = \langle M \rangle$ je lineární podprostor, ukazuje věta 2.37. Stačí ukázat, že P je nejmenší podprostor.

Nechť Q je nějaký podprostor, pro který také platí $M \subseteq Q$. Podle věty 2.37 je $\langle Q \rangle = Q$. Dále použijeme větu 2.34 na inkluzi $M \subseteq Q$ a dostáváme $P = \langle M \rangle \subseteq \langle Q \rangle = Q$.

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

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

Pro $\alpha_{n+1} \neq 0$ je vektor $\boldsymbol{z}$ lineární kombinací vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ (převedeme násobek vektoru $\boldsymbol{z}$ na druhou stranu rovnosti a podělíme $-\alpha_{n+1}$, jako v důkazu věty 2.21). To je ve sporu s tím, že $\boldsymbol{z} \notin \langle M \rangle$. Pro oba případy hodnot α_{n+1} dostáváme spor, takže $M \cup \{\boldsymbol{z}\}$ nemůže být lineárně závislá.

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

Důkaz (pro hloubavé čtenáře). Předpokládejme nejprve, že N je lineárně nezávislá. Nechť $M \subset N$, $M \neq N$. Zvolme vektor $\boldsymbol{z} \in N$ takový, že $\boldsymbol{z} \notin M$. Vektor $\boldsymbol{z}$ nelze vyjádřit jako lineární kombinaci žádné konečné podmnožiny prvků množiny M. Kdyby to bylo možné, tj. kdyby existovala $K \subseteq M$ konečná a taková, že $\boldsymbol{z}$ by byl roven lineární kombinaci prvků množiny K, pak je podle věty 2.21 množina $K \cup \{\boldsymbol{z}\} \subseteq N$ lineárně závislá. To je ve sporu s předpokladem, že N je lineárně nezávislá. Platí tedy, že $\boldsymbol{z} \notin \langle M \rangle$, a přitom $\boldsymbol{z} \in \langle N \rangle$.

Předpokládejme nyní, že N je lineárně závislá. Najdeme množinu $M \subset N$, $M \neq N$ takovou, že $\langle M \rangle = \langle N \rangle$. Protože N je lineárně závislá, existuje konečná množina vektorů $K_1 \subseteq N$, která je lineárně závislá. Podle věty 2.21 existuje prvek $\boldsymbol{z} \in K_1$ takový, že $\boldsymbol{z}$ lze zapsat jako lineární kombinaci ostatních vektorů z K_1. Zvolíme $M = N \setminus \{\boldsymbol{z}\}$ a dokážeme, že $\langle M \rangle = \langle N \rangle$. Je $\boldsymbol{z} \in \langle K_1 \setminus \{\boldsymbol{z}\} \rangle \subseteq \langle N \rangle$. Podle věty 2.35 vlastnosti (3) je $\langle N \rangle = \langle N \cup \{\boldsymbol{z}\} \rangle = \langle M \rangle$.

2.41. Poznámka. Abychom vyjádřili nějaký lineární (pod)prostor jako lineární obal nějaké množiny, je vhodné pro tento účel volit lineárně nezávislou množinu. Předchozí věta 2.40 nám ukazuje, že to je „nejúspornější opatření“, protože odebráním jakéhokoli prvku z takové množiny způsobí, že lineární obal už nebude pokrývat celý (pod)prostor. Žádné prvky takové množiny tedy nejsou při popisu (pod)prostoru pomocí lineárního obalu zbytečné. To nás vede (kromě jiných důležitých důvodů) k definici báze lineárního (pod)prostoru.

2.42. Definice. *Báze* lineárního prostoru L je taková podmnožina $B \subseteq L$, pro kterou platí *Báze*

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

2.43. Poznámka. V definici 2.42 se mluví o L jako o lineárním prostoru. Není ale vyloučeno, že L je lineární podprostor nějakého jiného (většího) lineárního prostoru P, protože lineární podprostor je podle poznámky 1.16 sám o sobě lineárním prostorem.

2.44. Příklad. Množina vektorů $B = \{(1,2,3), (1,0,2), (-2,1,0)\}$ je bází lineárního prostoru $\mathbf{R}^3$, protože je podle příkladu 2.13 lineárně nezávislá a podle příkladu 2.32 je $\langle B \rangle = \mathbf{R}^3$.

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

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

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

Všimněme si, že jsme už našli dvě báze lineárního prostoru $\mathbf{R}^3$ (v příkladu 2.44 a v tomto příkladu). Vidíme tedy, že báze není určena lineárním prostorem jednoznačně. Například pro $\alpha \neq 0$ jsou množiny $B_\alpha = \{\alpha\,(1,0,0), (0,1,0), (0,0,1)\}$ různé báze lineárního prostoru $\mathbf{R}^3$. Bází je tedy nekonečně mnoho.

2.46. Příklad. Množina uspořádaných n-tic $B = \{(1,0,0,\ldots,0), (0,1,0,\ldots,0), \ldots, (0,0,0,\ldots,0,1)\}$ tvoří bázi lineárního prostoru $\mathbf{R}^n$. Je lineárně nezávislá a platí $\langle B \rangle = \mathbf{R}^n$ z analogických důvodů, jako v příkladu 2.45. Takovou bázi lineárního prostoru $\mathbf{R}^n$ nazýváme *standardní bází.*

2.47. Příklad. Množina $B = \{1, x, x^2, x^3, \ldots\}$ tvoří bázi lineárního prostoru P všech polynomů. Podle příkladu 2.28 je lineárně nezávislá. Zbývá tedy ověřit, že $\langle B \rangle = P$. Zvolme nějaký polynom $p \in P$. Ukážeme, že $p \in \langle B \rangle$. Pro každý polynom $p \in P$ existuje $n \in \mathbf{N}$ a reálná čísla $a_0, a_1, \ldots, a_n$ taková, že hodnota polynomu p v bodě x je dána vzorcem

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

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

2.48. Příklad. Uvažujme lineární prostor $P_{\le n}$ všech polynomů nejvýše n-tého stupně z příkladu 1.19. Ukážeme, že množina $B_n = \{1, x, x^2, \ldots, x^n\}$ tvoří bázi lineárního prostoru $P_{\le n}$.

Předně, B_n je lineárně nezávislá, protože je podmnožinou lineárně nezávislé množiny B z příkladu 2.47 (každá podmnožina lineárně nezávislé množiny je podle poznámky 2.27 lineárně nezávislá). Analogicky jako v příkladu 2.47 lze ukázat, že $\langle B_n \rangle = P_{\le n}$.

2.49. Příklad. Vraťme se k lineárnímu prostoru U_O všech orientovaných úseček se společným počátkem. Podle (5) z příkladu 2.24 je každá lineárně nezávislá množina vektorů $\{\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}\}$ bází lineárního prostoru U_O.

2.50. Poznámka. *O existenci a jednoznačnosti báze.* Příklad 2.45 ilustroval skutečnost, že báze lineárního (pod)prostoru není určena jednoznačně. Lineární (pod)prostor může mít dokonce nekonečně mnoho bází.

Existenece a jednoznačnost báze

Následující věta dokládá, že každý lineární prostor má bázi. Výjimkou je pouze triviální lineární prostor $L = \{\boldsymbol{o}\}$, který jediný nemá bázi (někteří autoři uvádějí prázdnou množinu jako bázi triviálního lineárního prostoru, ovšem k tomu je potřeba mírně modifikovat definici lineárního obalu). Následující věta dokonce tvrdí, že každou lineárně nezávislou množinu lze doplnit přidáním případně dalších prvků na bázi a naopak, z každé množiny M, pro kterou $\langle M \rangle = L$, lze případně odebrat nějaké prvky tak, aby zbylá množina tvořila bázi. Větu bohužel nebudeme dokazovat, protože vyžaduje použití hlubších poznatků z teorie množin (tzv. Zornovo lemma), které v tuto chvíli nemáme k dispozici.

2.51. Věta. Nechť L je lineární prostor. Pro každou lineárně nezávislou množinu $N \subseteq L$ existuje báze B lineárního prostoru L taková, že $N \subseteq B$. Pro každou množinu $M \subseteq L$ takovou, že $\langle M \rangle = L$, existuje báze B lineárního prostoru L taková, že $B \subseteq M$.

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

Pokud už $\langle N \rangle = \mathbf{R}^n$, pak N samotná je báze a položíme $B = N$. Pokud ale $\langle N \rangle \ne \mathbf{R}^n$, pak existuje prvek $\boldsymbol{x} \in \mathbf{R}^n$, pro který $\boldsymbol{x} \notin \langle N \rangle$ Ptáme se, zda už $N \cup \{\boldsymbol{x}\}$ je báze. Podle věty 2.39 tato množina zůstává lineárně nezávislá. Pokud $\langle N \cup \{\boldsymbol{x}\} \rangle = \mathbf{R}^n$, pak jsme našli bázi. Jestliže tato vlastnost neplatí, opakujme postup s přidáním dalšího prvku $\boldsymbol{y} \notin \langle N \cup \{\boldsymbol{x}\} \rangle$ znovu. Tento postup budeme opakovat tak dlouho, dokud budou existovat vektory mimo lineární obal naší postupně rozšiřované množiny. Podle příkladu 2.20 dospějeme k výsledku po konečně mnoha krocích, protože v $\mathbf{R}^n$ nelze vytvořit lineárně nezávislou množinu, která by měla více než n prvků.

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

2.53. Příklad. Druhou část věty 2.51 si dokážeme aspoň pro konečnou množinu M. Je $\langle M \rangle = L$ a máme dokázat, že existuje $B \subseteq M$ taková, že $\langle B \rangle = L$ a navíc B je lineárně nezávislá.

Uvažujme všechny podmnožiny $A_i \subseteq M$, pro které $\langle A_i \rangle = L$. Vidíme, že existuje aspoň jedna taková podmnožina, sice množina M samotná. Ze všech takových podmnožin A_i vyberme tu, která má nejmenší počet prvků (všechny tyto podmnožiny jsou konečné, takže pro každou můžeme spočítat její počet prvků). Je možné, že takových množin s nejmenším počtem prvků bude existovat více, pak je jedno, kterou z nich zvolíme. Označme ji B. Víme, že $\langle B \rangle = L$ (tuto vlastnost mají všechny podmnožiny A_i, takže jmenovitě též množina B). Dále víme, že odebráním jakéhokoli prvku z množiny B už nebude pro novou B_1 platit $\langle B_1 \rangle = L$. Kdyby to platilo, tak nebyla vybrána B s nejmenším počtem prvků. Nyní použijeme větu 2.40. Množina B je tedy lineárně nezávislá.

2.54. Poznámka. Příklad báze prostoru F_D všech funkcí definovaných na množině $D \subset \mathbf{R}$ nebudeme uvádět, protože nemáme prostředky, jak takovou bázi zapsat. Báze je nekonečnou množinou, která má větší mohutnost, než je mohutnost množiny přirozených čísel.

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

Báze jsou stejně velké

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

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

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

Důkaz (pro hloubavé čtenáře). Použijeme matematickou indukci podle k (o indukci viz důkaz věty 4.3). Pro $k = 0$ věta platí, protože množinu M vůbec neměníme.

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

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

První rovnost je indukční předpoklad a druhá rovnost plyne z toho, že $\boldsymbol{v}_{k+1} \in \langle M \rangle = \langle M_1 \cup N_1 \rangle$ a z třetí vlastnosti věty 2.35. Stačí tedy najít v M_1 vektor $\boldsymbol{w}_1$ tak, aby jej šlo odebrat a obal se nezměnil, tedy $\langle M_1 \cup N \rangle = \langle M_1 \setminus \{\boldsymbol{w}_1\} \cup N \rangle$. Protože $\boldsymbol{v}_{k+1} \in \langle M \rangle = \langle M_1 \cup N_1 \rangle$, existuje konečně mnoho vektorů $\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_n \in M_1$ tak, že

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

Protože N je lineárně nezávislá, tak (A) při $k = 0$ musí být $\boldsymbol{v}_{k+1}$ nenulový a (B) při $k > 0$ nesmí $\boldsymbol{v}_{k+1}$ být lineární kombinací vektorů $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$ (věta 2.21). Z toho plyne, že $n > 0$ a nemohou být všechny koeficienty α_i nulové. Uspořádáme nyní $\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_n$ tak, aby $\alpha_1 \neq 0$. Z předchozí rovnosti plyne

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

takže $\boldsymbol{w}_1 \in \langle M_1 \setminus \{\boldsymbol{w}_1\} \cup N_1 \cup \{\boldsymbol{v}_{k+1}\} \rangle$. Podle (3) z věty 2.35 se přidáním vektoru $\boldsymbol{w}_1$ do množiny $M_1 \setminus \{\boldsymbol{w}_1\} \cup N$ lineární obal množiny nezmění, takže je $\langle M_1 \setminus \{\boldsymbol{w}_1\} \cup N \rangle = \langle M_1 \cup N \rangle = \langle M \rangle$. Uvedený postup přitom zaručil $\boldsymbol{w}_1 \in M_1$, takže z množiny M jsme celkem odebrali $k+1$ vektorů.

2.57. Poznámka. Steinitzova věta má následující důsledky.

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

Důkaz. Věta 2.56 tvrdí, že z množiny M lze odebrat tolik vektorů, kolik jich má množina N. Kdyby měla množina N více vektorů než množina M, pak by tento úkon nešel provést, tj. dostali bychom se do sporu se Steinitzovou větou.

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

Důkaz. Uvažujme dvě konečné báze B_1 a B_2 lineárního prostoru L. Protože $B_1 \subseteq \langle B_2 \rangle$ a B_1 je lineárně nezávislá, musí podle věty 2.58 mít B_2 aspoň tolik prvků, jako má B_1. Protože $B_2 \subseteq \langle B_1 \rangle$ a B_2 je lineárně nezávislá, musí podle stejné věty mít B_1 aspoň tolik prvků, jako má B_2. Takže počet prvků těchto množin musí být stejný.

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

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

2.61. Poznámka. Věta 2.59 nám zaručuje smysluplnost definice dimenze. Ačkoli lineární prostor může mít více bází, všechny tyto báze mají podle této věty stejný počet prvků, nebo jsou nekonečné. V tomto druhém případě klademe $\dim L = \infty$.

2.62. Příklad. $\dim \mathbf{R}^n = n$, viz příklad 2.46. $\dim P_{\le n} = n + 1$, viz příklad 2.48. $\dim P = \infty$, viz příklad 2.47. Konečně $\dim U_O = 3$ podle příkladu 2.49. Važme si toho, že nás Stvořitel obklopil lineárním prostorem dimenze 3 nejen proto, že trojka je šťastné číslo.

2.63. Věta. Nechť L je lineární prostor a $M \subseteq L$ je lineární podprostor lineárního prostoru L. Pak $\dim M \le \dim L$. *Dimenze podprostoru*

Důkaz. Označme B_L nějakou bázi lineárního prostoru L. Báze B_M množiny M je lineárně nezávislá množina, pro kterou je $B_M \subseteq \langle B_L \rangle$. Podle věty 2.58 má B_M nejvýše tolik prvků, jako B_L.

2.64. Věta. Nechť L je lineární prostor, $\dim L = n$ a $M = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m\}$. Pak platí: *Počet prvků v LN množině*
(1) Je-li M lineárně nezávislá, pak $m \le n$.
(2) Je-li $m > n$, pak M je lineárně závislá.
(3) Nechť $m = n$. Pak M je lineárně nezávislá právě tehdy, když $\langle M \rangle = L$.

Důkaz. (1) Množinu M lze doplnit podle věty 2.51 na případně větší množinu B, která je bází. Tato množina má podle věty 2.59 vždy n prvků. Protože $M \subseteq B$, musí $m \le n$.

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

(3) Nechť nejprve M je lineárně nezávislá. Kdyby $\langle M \rangle \ne L$, pak lze přidat do množiny M vektor $\boldsymbol{x} \notin \langle M \rangle$, a přitom podle věty 2.39 zůstane rozšířená množina lineárně nezávislá. To ale podle (1) není možné. Musí tedy $\langle M \rangle = L$. Předpokládejme nyní, že M je lineárně závislá. Kdyby $\langle M \rangle = L$, pak podle věty 2.51 existuje báze $B \subseteq M$, a přitom B bude mít méně prvků než množina M (protože M je lineárně závislá). To podle věty 2.59 není možné, neboť každá báze má n prvků. Musí tedy $\langle M \rangle \ne L$.

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

2.66. Příklad. Množina $\{(1,1,1), (0,1,1), (0,0,2)\}$ je bází lineárního prostoru $\mathbf{R}^3$, protože je lineárně nezávislá a její počet prvků je roven $\dim \mathbf{R}^3$. Stačí použít větu 2.64, vlastnost (3) a nemusíme pracně ověřovat z definice, že lineární obal této množiny pokrývá celé $\mathbf{R}^3$.

3. Matice

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

3.1. Definice. *Matice typu* (m, n) je uspořádaná m-tice prvků z $\mathbf{R}^n$. Jednotlivé složky této m-tice nazýváme *řádky matice*. Nechť $\boldsymbol{a}_r = (a_{r,1}, a_{r,2}, \ldots, a_{r,n})$ je r-tý řádek matice typu (m, n). s-tá složka tohoto řádku $a_{r,s} \in \mathbf{R}$ se nazývá (r, s)*-tý prvek* matice. Řádky matice $\mathbf{A}$ zapisujeme jako skutečné řádky pod sebe takto: *Definice matice*

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

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

$$\mathbf{A} = (a_{r,s}), \quad r \in \{1, 2, \ldots, m\}, \, s \in \{1, 2, \ldots, n\}.$$

Nechť $\mathbf{A} = (a_{r,s}), r \in \{1, \ldots, m\}, s \in \{1, \ldots, n\}$. Uspořádanou m-tici reálných čísel $(a_{1,s}, a_{2,s}, \ldots, a_{m,s})$ nazýváme *s-tým sloupcem matice* $\mathbf{A}$.

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

Matici typu (m, n) nazýváme *čtvercovou maticí*, pokud $m = n$.

3.2. Poznámka. Dvě matice se rovnají, pokud jsou stejného typu a všechny prvky jedné matice se rovnají odpovídajícím prvkům matice druhé. To vyplývá z definice: rovnost dvou uspořádaných m-tic řádků z $\mathbf{R}^n$ je definována tak, že všechny složky první m-tice se rovnají odpovídajícím složkám druhé m-tice, jinými slovy odpovídající řádky se rovnají. Rovnost řádků jako uspořádaných n-tic reálných čísel je definována tak, že se odpovídající složky těchto řádků rovnají.

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

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

3.4. Věta. Množina všech matic shodného typu (m, n) tvoří se sčítáním matic a násobením matice reálným číslem podle definice 3.3 lineární prostor. Nulový vektor tohoto prostoru je nulová matice.

Důkaz. Důkaz si čtenář provede sám jako cvičení. Srovnejte s příklady 1.9 a 1.11.

3.5. Příklad. Množina

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

tvoří bázi lineárního prostoru $M_{3,2}$ všech matic typu $(3, 2)$.

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

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

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

Ověříme nyní vlastnost (2) z definice 2.42. Nechť

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

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

Dimenze lineárního prostoru $M_{3,2}$ je podle definice 2.60 rovna šesti.

3.6. Příklad. Je-li $M_{m,n}$ lineární prostor všech matic typu (m, n), pak $\dim M_{m,n} = m \cdot n$. Analogicky jako v příkladu 3.5 lze totiž sestrojit bázi lineárního prostoru $M_{m,n}$, která má $m \cdot n$ prvků.

3.7. Poznámka. Na matice můžeme pohlížet jako na prvky lineárního prostoru, protože je umíme sčítat a násobit reálným číslem. Kromě toho se ale naučíme s maticemi dělat další kousky. Například umíme řádky matice modifikovat způsobem, jaký jsme se naučili při Gaussově eliminační metodě. V následující části textu ukážeme, že modifikace matice podle Gaussovy eliminační metody má několik velmi důležitých vlastností s praktickými důsledky.

3.8. Poznámka. Protože řádky matice typu (m, n) jsou podle definice 3.1 prvky lineárního prostoru $\mathbf{R}^n$, umíme je sčítat, násobit reálným číslem, rozhodovat o jejich lineární nezávislosti, sestrojovat lineární obaly, podprostory, hledat báze, dimenze apod.

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

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

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

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

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

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

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

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

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

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

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

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

Gaussova eliminace zachovává obal

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

Všechny řádky matice $\mathbf{A}_1$ lze zapsat jako lineární kombinaci řádků matice $\mathbf{A}$. Je přitom jedno, zda matice $\mathbf{A}_1$ vznikla prohozením řádků, pronásobením jednoho řádku nenulovým reálným číslem, přičtením násobku jednoho řádku k jinému, odebráním nebo přidáním nulového řádku. Platí tedy, že řádky matice $\mathbf{A}_1$ leží v $\langle \mathrm{r}\colon \mathbf{A}\rangle$. Proto $\langle \mathrm{r}\colon \mathbf{A}_1\rangle \subseteq \langle\langle \mathrm{r}\colon \mathbf{A}\rangle\rangle$. Podle věty 2.35 je $\langle\langle \mathrm{r}\colon \mathbf{A}\rangle\rangle = \langle \mathrm{r}\colon \mathbf{A}\rangle$, takže $\langle \mathrm{r}\colon \mathbf{A}_1\rangle \subseteq \langle \mathrm{r}\colon \mathbf{A}\rangle$.

Pomocné tvrzení máme dokázáno. Pokud toto tvrzení uplatníme opakovaně (matice $\mathbf{B}$ vznikla z matice $\mathbf{A}$ po konečně mnoha krocích podle Gaussovy eliminační metody), máme výsledek $\langle \mathrm{r}\colon \mathbf{B}\rangle \subseteq \langle \mathrm{r}\colon \mathbf{A}\rangle$. Tvrzení dokazované věty nyní plyne ze symetrie relace „$\sim$“, tj. z věty 3.10.

3.14. Příklad. Řádky matice $\mathbf{A}$ i matice $\mathbf{B}$ uvedené níže mají podle věty 3.13 stejné lineární obaly. Tyto obaly tvoří podle věty 2.37 nějaký lineární podprostor lineárního prostoru $\mathbf{R}^5$.

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

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

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

Hodnost matice

3.16. Příklad. Matice $\mathbf{A}$ z příkladu 3.14 má hodnost 3.

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

Důkaz. Věta je jednoduchým důsledkem věty 3.13 a definice 3.15.

3.18. Věta. Hodnost matice je maximální počet lineárně nezávislých řádků matice. Přesněji řečeno, hodnost udává počet prvků takové množiny řádků, která je nejpočetnější, a přitom lineárně nezávislá.

Důkaz. Jak jsme již řekli v poznámce 2.65, báze podprostoru $\langle \mathrm{r}\colon \mathbf{A}\rangle$ je nejpočetnější lineárně nezávislá množina. Tedy $\mathrm{hod}\,\mathbf{A} = \dim\langle \mathrm{r}\colon \mathbf{A}\rangle =$ počet prvků báze lineárního prostoru $\langle \mathrm{r}\colon \mathbf{A}\rangle$.

3.19. Poznámka. Například ve skriptech [7] je hodnost matice definována jako maximální počet lineárně nezávislých řádků matice. Pro důkaz věty 3.17 je v těchto skriptech vyvinuto poněkud větší úsilí, protože se tento důkaz neopírá o pojmy lineární obal a o výsledky z kapitoly 2.0.

3.20. Poznámka. Matice $\mathbf{B}$ v příkladu 3.14 je typickou ukázkou matice, která vznikne po ukončení přímého chodu Gaussovy eliminační metody. Jedná se o matici, ve které každý následující řádek má aspoň o jednu nulu v souvislé řadě nul (psané z leva) více, než řádek předchozí. Přitom matice neobsahuje nulové řádky. Takovým maticím budeme říkat horní trojúhelníkové (nenulové prvky jsou jen v „pásmu horního trojúhelníka“).

Trojúhelníkové matice

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

3.22. Věta. Horní trojúhelníková matice má vždy lineárně nezávislé řádky.

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

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

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

3.23. Věta. Každou matici lze převést konečným počtem kroků Gaussovy eliminační metody na horní trojúhleníkovou matici.

Důkaz. Plyne z popisu přímého chodu Gaussovy eliminační metody.

3.24. Poznámka. Tato věta nám společně s větou 3.13 dává záruky, že hodnost libovolné matice můžeme spočítat postupem, jaký jsme zvolili v příkladu 3.14.

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

3.26. Poznámka. Postup přímého chodu Gassovy eliminační metody podle poznámky 3.25 se může hodit ve dvou případech.

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

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

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

$$\mathbf{C} = \begin{pmatrix} 28{,}33333 & 11{,}33333 \\ 56{,}66667 & 22{,}66666 \end{pmatrix},$$

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

Problematiku numerických metod v tuto chvíli opustíme, protože není obsahem tohoto předmětu.

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

3.29. Příklad.

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

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

Důkaz. Věta plyne přímo z definice 3.28.

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

Důkaz (pro hloubavé čtenáře). Ukážeme nejprve, že $\mathrm{hod}(\mathbf{A}^T) \geq \mathrm{hod}(\mathbf{A})$. Nechť $\mathbf{A}$ je typu (m, n) a označme $k = \mathrm{hod}(\mathbf{A})$. Podle věty 3.18 existuje k lineárně nezávislých řádků matice $\mathbf{A}$. Označme je $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$. Zapišme si, co to znamená, že tyto řádky jsou lineárně nezávislé. Pro

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

musí být $\alpha_i = 0 \;\forall i \in \{1, \ldots, k\}$. Tento požadavek vede na soustavu rovnic, která musí mít jedině triviální řešení:

$$\begin{aligned} \alpha_1 \, b_{1,1} + \alpha_2 \, b_{2,1} + \cdots + \alpha_k \, b_{k,1} \; &= 0, \\ \alpha_1 \, b_{1,2} + \alpha_2 \, b_{2,2} + \cdots + \alpha_k \, b_{k,2} \; &= 0, \\ \cdots \\ \alpha_1 \, b_{1,n} + \alpha_2 \, b_{2,n} + \cdots + \alpha_k \, b_{k,n} \; &= 0. \end{aligned} \tag{3.1}$$

Koeficienty jednotlivých rovnic soustavy (3.1) odpovídají částem sloupců matice $\mathbf{A}$. Částmi sloupců v tomto důkazu budeme označovat uspořádané k-tice obsahující jen ty prvky z daného sloupce, které leží ve vybraných řádcích $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$. Aby bylo zaručeno pouze triviální řešení soustavy (3.1), musíme po přímém chodu Gaussovy eliminační metody dostat trojúhelníkovou matici o k-řádcích (méně řádků by vedlo na nekonečně mnoho řešení). To podle vět 3.18 a 3.13 znamená, že existuje k lineárně nezávislých částí sloupců matice $\mathbf{A}$. Tytéž celé sloupce matice $\mathbf{A}$ jsou lineárně nezávislé (kdyby byly závislé, pak by stejná netriviální lineární kombinace celých sloupců dávala nulový vektor i na částech sloupců, ale my víme, že části sloupců jsou lineárně nezávislé). Máme tedy zaručeno, že v matici $\mathbf{A}$ je aspoň k lineárně nezávislých sloupců (zatím není vyloučeno, že jich může být více). Podle věty 3.18 tedy je $\mathrm{hod}(\mathbf{A}^T) \geq k = \mathrm{hod}(\mathbf{A})$.

Máme $\mathrm{hod}\big((\mathbf{A}^T)^T\big) \geq \mathrm{hod}(\mathbf{A}^T) \geq \mathrm{hod}(\mathbf{A})$, a přitom podle věty 3.30 je $(\mathbf{A}^T)^T = \mathbf{A}$, takže všechny uvedené hodnosti se rovnají.

3.32. Poznámka. Ukázali jsme, že hodnosti matice $\mathbf{A}$ a $\mathbf{A}^T$ se rovnají. To vysvětluje, proč jsme nedefinovali zvlášť „řádkovou" hodnost matice jako dimenzi lineárního obalu řádků a zvlášť „sloupcovou" hodnost jako dimezi lineárního obalu sloupců. Tato čísla jsou podle věty 3.31 stejná.

3.33. Věta. Nechť $\mathbf{A}$ je matice typu (m, n). Pak $\mathrm{hod}(\mathbf{A}) \leq \min(m, n)$.

Důkaz. Hodnost matice je menší nebo rovna počtu řádků z věty 3.18 a je menší nebo rovna počtu sloupců z věty 3.31.

3.34. Definice. Nechť $\mathbf{A} = (a_{i,j})$ je matice typu (m, n) a $\mathbf{B} = (b_{j,k})$ je matice typu (n, p). Pak je definován *součin matic* $\mathbf{A} \cdot \mathbf{B}$ (v tomto pořadí) jako matice typu (m, p) takto: každý prvek $c_{i,k}$ matice $\mathbf{A} \cdot \mathbf{B}$ je dán vzorcem *Násobení matic*

$$c_{i,k} = a_{i,1} \, b_{1,k} + a_{i,2} \, b_{2,k} + \cdots + a_{i,n} \, b_{n,k} = \sum_{j=1}^{n} a_{i,j} \, b_{j,k}, \quad i \in \{1, \ldots, m\}, \quad k \in \{1, \ldots, p\}. \tag{3.2}$$

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

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

Každý prvek matice $\mathbf{A} \cdot \mathbf{B}$ přitom musíme počítat podle vzorce (3.2) jako součet součinů odpovídajících prvků řádku první matice a sloupce druhé matice. Začátečníci mohou použít tzv. „dvouprstovou vizuální metodu": při výpočtu čísla $c_{i,k}$ přiložte ukazováček levé ruky na začátek i-tého řádku první matice a ukazováček pravé ruky na začátek k-tého sloupce druhé matice. Pak pronásobte mezi sebou čísla, na která ukazují prsty, a výsledek uložte do sčítací paměti. Posuňte levý prst na další prvek v řádku a pravý prst na další prvek v sloupci. Znovu vynásobte a přičtěte výsledek ke sčítací paměti. Posunujte dále levý prst v řádku a pravý prst ve sloupci, násobte a sčítejte ve sčítací paměti tak dlouho, dokud nevyčerpáte celý řádek první matice. To se stane podle definice v okamžiku, kdy též vyčerpáte celý sloupec druhé matice. Výsledek sčítací paměti pak napište jako prvek $c_{i,k}$ do postupně budované výsledné matice $\mathbf{A} \cdot \mathbf{B}$.

3.36. Příklad.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 0 & 2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \\ 2 & 7 \end{pmatrix} = \begin{pmatrix} 1\cdot 1+2\cdot 3+3\cdot 5+4\cdot 2 & 1\cdot 2+2\cdot 4+3\cdot 6+4\cdot 7 \\ 5\cdot 1+6\cdot 3+7\cdot 5+8\cdot 2 & 5\cdot 2+6\cdot 4+7\cdot 6+8\cdot 7 \\ 0\cdot 1+2\cdot 3+1\cdot 5+0\cdot 2 & 0\cdot 2+2\cdot 4+1\cdot 6+0\cdot 7 \end{pmatrix} = \begin{pmatrix} 30 & 56 \\ 74 & 132 \\ 11 & 14 \end{pmatrix}.$$

3.37. Příklad.

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

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

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

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

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

3.38. Věta. Nechť $\alpha \in \mathbf{R}$ a matice $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ jsou odpovídajících typů tak, aby níže uvedené součiny a součty byly definovány. Pak platí

(1) $(\mathbf{A}\cdot\mathbf{B})\cdot\mathbf{C} = \mathbf{A}\cdot(\mathbf{B}\cdot\mathbf{C})$ (asociativní zákon),
(2) $(\mathbf{A}+\mathbf{B})\cdot\mathbf{C} = \mathbf{A}\cdot\mathbf{C}+\mathbf{B}\cdot\mathbf{C}$ (distributivní zákon),
(3) $\mathbf{C}\cdot(\mathbf{A}+\mathbf{B}) = \mathbf{C}\cdot\mathbf{A}+\mathbf{C}\cdot\mathbf{B}$ (distributivní zákon),
(4) $\alpha(\mathbf{A}\cdot\mathbf{B}) = (\alpha\,\mathbf{A})\cdot\mathbf{B} = \mathbf{A}\cdot(\alpha\,\mathbf{B})$,
(5) $(\mathbf{A}\cdot\mathbf{B})^T = \mathbf{B}^T\cdot\mathbf{A}^T$.

Důkaz. Jako cvičení doplňte ke každému vzorci věty předpoklady o typech matic. Tyto předpoklady se budou pro různé vzorce lišit. V tomto důkazu předpokládáme typy matic (m,n), (n,p) a (p,q).

(1) Označme $\mathbf{A} = (a_{i,j})$, $\mathbf{B} = (b_{j,k})$, $\mathbf{C} = (c_{k,l})$, $\mathbf{A}\cdot\mathbf{B} = (d_{i,k})$, $\mathbf{B}\cdot\mathbf{C} = (f_{j,l})$, $(\mathbf{A}\cdot\mathbf{B})\cdot\mathbf{C} = (g_{i,l})$, $\mathbf{A}\cdot(\mathbf{B}\cdot\mathbf{C}) = (h_{i,l})$ pro $i \in \{1,\ldots,m\}$, $j \in \{1,\ldots,n\}$, $k \in \{1,\ldots,p\}$, $l \in \{1,\ldots,q\}$. Jde o to ukázat, že $g_{i,l} = h_{i,l}$ pro všechna $i \in \{1,\ldots,m\}$ a $l \in \{1,\ldots,q\}$. Podle definice 3.34 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 $a_{i,j}\cdot b_{j,k}\cdot c_{k,l}$ můžeme zapsat do tabulky, ve které index j odpovídá řádku tabulky a index k sloupci. Hodnota X pak znamená součet sloupcových mezisoučtů v tabulce a hodnota Y součet řádkových mezisoučtů. Každá účetní ví, že obě hodnoty musí dát stejný výsledek. My ostatní to snadno nahlédneme.

(2) Označme $\mathbf{A} = (a_{i,j})$, $\mathbf{B} = (b_{i,j})$, $\mathbf{C} = (c_{j,k})$, $(\mathbf{A}+\mathbf{B})\cdot\mathbf{C} = (d_{i,k})$ pro $i \in \{1,\ldots,m\}$, $j \in \{1,\ldots,n\}$, $k \in \{1,\ldots,p\}$. Pak podle definic 3.34 a 3.3 platí

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

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

(3) Důkaz bychom provedli obdobně, jako v případě (2).

(4) Označme $\mathbf{A}=(a_{i,j})$, $\mathbf{B}=(b_{j,k})$ pro $i\in\{1,\dots,m\}$, $j\in\{1,\dots,n\}$, $k\in\{1,\dots,p\}$. Platí

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

což dokazuje vzorec: (4).

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

$$c_{i,k}=\sum_{j=1}^{n}a_{i,j}\,b_{j,k}=\sum_{j=1}^{n}\beta_{k,j}\,\alpha_{j,i}=d_{k,i},$$

takže $\mathbf{D}^T=\mathbf{C}$, což dokazuje vzorec (5).

3.39. Příklad. Nechť $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ jsou čtercové matice. Spočítáme $(\mathbf{A}+\mathbf{B})\cdot(\mathbf{B}+\mathbf{C})$. Podle (3) ve větě 3.38 je $(\mathbf{A}+\mathbf{B})\cdot(\mathbf{B}+\mathbf{C})=(\mathbf{A}+\mathbf{B})\cdot\mathbf{B}+(\mathbf{A}+\mathbf{B})\cdot\mathbf{C}=\mathbf{A}\cdot\mathbf{B}+\mathbf{B}\cdot\mathbf{B}+\mathbf{A}\cdot\mathbf{C}+\mathbf{B}\cdot\mathbf{C}$. Místo zápisu $\mathbf{B}\cdot\mathbf{B}$ budeme užívat zkratku $\mathbf{B}^2$. Konečný výsledek je $\mathbf{A}\cdot\mathbf{B}+\mathbf{B}^2+\mathbf{A}\cdot\mathbf{C}+\mathbf{B}\cdot\mathbf{C}$.

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

3.40. Příklad. Nechť je dána čtercová matice $\mathbf{A}$ typu (n,n). Pokud matice $\mathbf{B}$ splňuje rovnost $\mathbf{A}\cdot\mathbf{B}=\mathbf{B}\cdot\mathbf{A}$, říkáme, že matice $\mathbf{B}$ *komutuje* s maticí $\mathbf{A}$. Ukážeme, že množina všech komutujících matic s danou maticí $\mathbf{A}$ tvoří lineární podprostor lineárního prostoru všech matic typu (n,n).

Komutující matice

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

Podle definice 1.17 stačí ukázat, že pokud jsou $\mathbf{B}$ a $\mathbf{C}$ komutující matice s maticí $\mathbf{A}$ a $\alpha\in\mathbf{R}$, pak též $\mathbf{B}+\mathbf{C}$ a $\alpha\,\mathbf{B}$ jsou komutující matice. Předpokládejme tedy, že platí $\mathbf{A}\cdot\mathbf{B}=\mathbf{B}\cdot\mathbf{A}$, $\mathbf{A}\cdot\mathbf{C}=\mathbf{C}\cdot\mathbf{A}$. V následujícím výpočtu použijeme věty 3.38, vzorce (2) až (4) a našeho předpokladu.

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

3.41. Příklad. Najdeme bázi a dimenzi lineárního podprostoru M všech matic komutujících s maticí

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

Podle předchozího příkladu musejí být matice komutující s maticí $\mathbf{A}$ rovněž typu $(2,2)$. Předpokládejme, že matice $\mathbf{B}$ lze zapsat ve tvaru

$$\mathbf{B}=\begin{pmatrix}a&b\\c&d\end{pmatrix}.$$

Jednotlivé součiny pak vypadají následovně

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

Tyto součiny se mají rovnat. Podle poznámky 3.2 se dvě matice rovnají, pokud se vzájemně rovnají všechny jejich odpovídající prvky. To nás vede ke čtyřem rovnicím o čtyřech neznámých, které upravíme Gaussovou elmininační metodou.

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

Proměnné c a d můžeme volit libovolně. Uvedené dvě rovnice nám umožňují dopočítat proměnné b a a takto: $b = 2/3\,c$, $a = d-c$. Všechny matice, které komutují s maticí $\mathbf{A}$ jsou tedy určeny dvěma parametry:

$$\mathbf{B} = \begin{pmatrix} d-c & \frac{2}{3}c \\ c & d \end{pmatrix} = c\begin{pmatrix} -1 & \frac{2}{3} \\ 1 & 0 \end{pmatrix} + d\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad c \in \mathbf{R}, \quad d \in \mathbf{R}.$$

Lineární prostor všech komutujících matic M se nám podařilo vyjádřit jako množinu všech lineárních kombinací dvou konstantních matic. Tuto skutečnost zapíšeme pomocí lineárního obalu takto:

$$M = \left\langle \begin{pmatrix} -1 & \frac{2}{3} \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} -3 & 2 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle.$$

Poslední úpravu (pronásobení první matice třemi) jsme nemuseli dělat, pokud se spokojíme se zlomkem ve výsledku. V modelových příkladech se dosti často snažíme dostat výsledek vyjádřitelný v malých celých číslech. Není to samozřejmě naší povinností, pouze pak výsledek lépe vypadá a nás více potěší.

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

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

3.42. Poznámka. V definici 3.1 jsme zavedli matice, jejíž prvky jsou reálná čísla. Občas se ale setkáme s maticemi, jejíž prvky jsou vektory, tedy prvky libovolného lineárního prostoru. Za *matici vektorů* typu (m,n) budeme považovat uspořádanou m-tici prvků z L^n, kde L je nějaký lineární prostor a znakem L^n zde označujeme množinu uspořádaných n-tic prvků z L. Protože lze prvky lineárního prostoru podle definice 1.6 násobit reálným číslem, lze přirozeně definovat též maticové násobení $\mathbf{A}\cdot\mathbf{B}$, kde $\mathbf{A} = (a_{i,j})$ je matice reálných čísel typu (m,n) a $\mathbf{B} = (\boldsymbol{b}_{j,k})$ je matice vektorů typu (n,p). Výsledná matice $\mathbf{A}\cdot\mathbf{B}$ je maticí vektorů typu (m,p) s prvky $\boldsymbol{c}_{i,k}$, pro které platí: *Matice vektorů*

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

3.43. Příklad. Nechť $\mathbf{A}$ je matice reálných čísel typu $(1,n)$ a $\mathbf{B}$ je matice vektorů typu $(n,1)$. Pak součin $\mathbf{A}\cdot\mathbf{B}$ je lineární kombinace vektorů z $\mathbf{B}$, přičemž prvky z $\mathbf{A}$ jsou koeficienty této lineární kombinace. Názorně:

$$(\,a_1, \quad a_2, \quad \cdots, \quad a_n\,)\cdot\begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \\ \vdots \\ \boldsymbol{b}_n \end{pmatrix} = a_1\,\boldsymbol{b}_1 + a_2\,\boldsymbol{b}_2 + \cdots + a_n\,\boldsymbol{b}_n.$$

3.44. Definice. Čtvercovou matici $\mathbf{E}$ typu (n,n) nazýváme *jednotkovou maticí*, pokud pro její prvky $e_{i,j}$ platí: $e_{i,j} = 0$ pro $i \ne j$ a $e_{i,j} = 1$ pro $i = j$. Názorně: *Jednotková matice*

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

3.45. Poznámka. Z definice maticového násobení okamžitě plyne, že pro každou čtvercovou matici $\mathbf{A}$ typu (n,n) je $\mathbf{E}\cdot\mathbf{A} = \mathbf{A}\cdot\mathbf{E} = \mathbf{A}$. Jednotková matice má tedy stejnou vlastnost vzhledem k násobení, jako jednička při násobení reálných čísel. Pro reálná čísla taky platí, že $1\cdot a = a\cdot 1 = a$.

Všimneme si také, že jednotková matice je komutující s každou čtvercovou maticí.

3.46. Poznámka. Vraťme se k příkladu 3.41. Tam jsme našli bázi, ve které je jednotková matice. To nás nepřekvapí, protože jednotková matice je komutující s každou maticí. Dále s maticí $\mathbf{A}$ komutuje stejná matice $\mathbf{A}$. Pokud víme, že $\dim M = 2$ a matice $\mathbf{A}$ a $\mathbf{E}$ jsou lineárně nezávislé, můžeme rovnou prohlásit, že hledaná báze lineárního podprostoru M je $\{\mathbf{A}, \mathbf{E}\}$. Zdálo by se, že jsme výpočty v příkladu 3.41 dělali zbytečně. Není to tak docela pravda, protože dopředu nevíme, zda dimenze hledaného prostoru bude rovna dvěma.

3.47. Poznámka. V definici 3.44 jsme zavedli jednotkovou matici s podobnými vlastnostmi, jako má reálné číslo 1. Vraťme se znovu ke srovnání s reálnými čísly. Pro každé nenulové reálné číslo a existuje reálné číslo b takové, že $ab = 1$. Takové reálné číslo obvykle nazýváme převrácenou hodnotou čísla a a označujeme $1/a$ nebo též a^{-1}. Analogicky definujeme „převrácenou hodnotu matice“, tzv. inverzní matici.

Inverzní matice

3.48. Definice. Nechť $\mathbf{A}$ je čtvercová matice typu (n,n) a $\mathbf{E}$ je jednotková matice stejného typu. Matici $\mathbf{B}$ typu (n,n), která splňuje vlastnost $\mathbf{A}\cdot\mathbf{B} = \mathbf{E} = \mathbf{B}\cdot\mathbf{A}$ nazýváme *inverzní maticí* k matici $\mathbf{A}$. Inverzní matici k matici $\mathbf{A}$ označujeme symbolem $\mathbf{A}^{-1}$.

3.49. Věta. Pokud k matici $\mathbf{A}$ existuje inverzní matice, pak je tato inverzní matice jednoznačně určena.

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

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

Zde jsme po řadě využili: poznámku 3.45, vlastnost, že $\mathbf{C}$ je inverzní matice k $\mathbf{A}$, vlastnost (1) z věty 3.38, vlastnost, že $\mathbf{B}$ je inverzní matice k $\mathbf{A}$, a konečně znovu poznámku 3.45.

3.50. Věta. Ke čtvercové matici typu (n,n) existuje inverzní matice právě tehdy, když $\mathrm{hod}(\mathbf{A}) = n$.

Důkaz. Důkaz této věty přesuneme až do příští kapitoly o determinantech. Věta ukazuje, že matice, které mají hodnost rovnu počtu řádků (tj. podle věty 3.18 jsou všechny řádky lineárně nezávislé) mají inverzní matici. Pokud jsou řádky lineárně závislé, inverzní matice neexistuje. Můžeme tedy říci, že pokud jsou řádky ve čtvercové matici lineárně závislé, je matice z hlediska maticového násobení „skoro nulová“ v tom smyslu, že k ní neexistuje inverzní matice (podobně jako k reálnému číslu nula neexistuje převrácená hodnota). To nás inspiruje k následující definici.

3.51. Definice. Čtvercová matice $\mathbf{A}$ typu (n,n) se nazývá *regulární*, pokud $\mathrm{hod}(\mathbf{A}) = n$. Čtvercová matice $\mathbf{A}$ se nazývá *singulární*, pokud není regulární, tj. $\mathrm{hod}(\mathbf{A}) < n$.

Regulární, singulární matice

3.52. Věta. Nechť $\mathbf{A}$ a $\mathbf{B}$ jsou regulární čtvercové matice typu (n,n). Pak matice $\mathbf{A}\cdot\mathbf{B}$ je rovněž regulární matice typu (n,n).

Důkaz. Matice $\mathbf{A}\cdot\mathbf{B}$ je čtvercová typu (n,n). To plyne přímo z definice maticového součinu. Stačí tedy dokázat, že je regulární. Podle věty 3.50 je matice regulární právě tehdy, když k ní existuje inverzní matice. Podle předpokladu k matici $\mathbf{A}$ existuje inverzní matice $\mathbf{A}^{-1}$ a k matici $\mathbf{B}$ existuje inverzní matice $\mathbf{B}^{-1}$. Stačí ukázat, že existuje inverzní matice k matici $\mathbf{A}\cdot\mathbf{B}$. Hledaná inverzní matice je tvaru $\mathbf{B}^{-1}\cdot\mathbf{A}^{-1}$, protože:

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

3.53. Příklad. Nejprve na jednoduchém příkladu ukážeme obvyklý postup hledání inverzní matice k dané matici $\mathbf{A}$. Teprve pak dokážeme, že tento postup je oprávněný a vždy vede k inverzní matici.

Výpočet inverzní matice eliminací

Naším úkolem bude najít inverzní matici k matici

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ -1 & 0 & 1 \\ 2 & 2 & 1 \end{pmatrix}.$$

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

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

Tvrdíme, že hledaná inverzní matice k matici $\mathbf{A}$ je zapsána vpravo od svislé čáry v poslední úpravě. Přesněji, pokud $(\mathbf{A}|\mathbf{E}) \sim (\mathbf{E}|\mathbf{B})$, kde „$\sim$“ znamená konečně mnoho řádkových úprav matice podle Gaussovy eliminační metody, pak $\mathbf{B} = \mathbf{A}^{-1}$.

Zvídavý student se oprávněně ptá, proč tato metoda dává inverzní matici. Než si na to odpovíme, budeme muset propočítat následující příklad a dokázat dvě následující věty.

3.54. Příklad. Nechť $\mathbf{A}$ je matice typu (m,n). Nechť dále $\mathbf{P}_1$ je čtvercová matice typu (m,m), která vznikne z matice $\mathbf{E}$ prohozením i-tého řádku s j-tým. Pak matice $\mathbf{B} = \mathbf{P}_1 \cdot \mathbf{A}$ je shodná s maticí $\mathbf{A}$ až na to, že má přehozený i-tý řádek s j-tým. Rozmyslete si to sami.

Nechť $\mathbf{P}_2$ je čtvercová matice typu (m,m), která vznikne z matice $\mathbf{E}$ pronásobením i-tého řádku číslem α. Pak matice $\mathbf{B} = \mathbf{P}_2 \cdot \mathbf{A}$ je shodná s maticí $\mathbf{A}$ až na to, že má pronásobený i-tý řádek číslem α. Ověřte si to sami.

Nechť konečně $\mathbf{P}_3$ je čtvercová matice typu (m,m), která vznikne z matice $\mathbf{E}$ záměnou jednoho nulového prvku na zvolené pozici i,j $(i \neq j)$ číslem α. Pak matice $\mathbf{B} = \mathbf{P}_2 \cdot \mathbf{A}$ je shodná s maticí $\mathbf{A}$ až na to, že místo i-tého řádku je zde zapsán součet i-tého řádku matice $\mathbf{A}$ s α-násobkem j-tého řádku. Prověřte si to sami.

Z předchozího vidíme, že jednotlivé kroky Gaussovy eliminační metody můžeme „emulovat“ násobením vhodné čtvercové matice zleva. Následné použití dalších kroků lze „emulovat“ násobením dalšími čtvercovými maticemi zleva. Tento poznatek precizuje následující věta.

3.55. Věta. Nechť $\mathbf{A} \sim \mathbf{B}$ jsou dvě matice, přičemž v eliminaci označené zde symbolem „$\sim$“ nebyl použit krok vynechání nebo přidání nulového řádku. Pak existuje regulární čtvercová matice $\mathbf{P}$ taková, že $\mathbf{B} = \mathbf{P} \cdot \mathbf{A}$.

Důkaz. Pro jednotlivé kroky Gaussovy eliminační metody jsme našli odpovídající čtvercové matice v příkladu 3.54. Vznikla-li matice $\mathbf{B}$ po k krocích Gaussovy eliminační metody, pak zřejmě existují matice $\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_k$ (každá z nich je některého ze tří typů podle příkladu 3.54) takové, že

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

Zde jsme využili asociativního zákona pro násobení matic z věty 3.38.

Výsledná matice $\mathbf{P}$ je regulární, protože všechny matice $\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_k$ jsou regulární (mají lineárně nezávislé řádky) a součin regulárních matic je regulární podle věty 3.52.

3.56. Věta. Nechť $\mathbf{A}$ je regulární a $(\mathbf{A}|\mathbf{E}) \sim (\mathbf{E}|\mathbf{B})$, kde „$\sim$“ označuje konečný počet řádkových úprav podle eliminační metody a $\mathbf{E}$ jednotkovou matici. Pak $\mathbf{B} = \mathbf{A}^{-1}$.

Důkaz. Podle věty 3.55 existuje čtvercová matice $\mathbf{P}$ taková, že

$$(\mathbf{A} \,|\, \mathbf{E}) \sim (\mathbf{E} \,|\, \mathbf{B}) = (\mathbf{P} \cdot \mathbf{A} \,|\, \mathbf{P} \cdot \mathbf{E}).$$

Protože $\mathbf{P} \cdot \mathbf{A} = \mathbf{E}$, je matice $\mathbf{P}$ inverzní maticí k matici $\mathbf{A}$. Protože $\mathbf{B} = \mathbf{P} \cdot \mathbf{E}$, je matice $\mathbf{B}$ přímo rovna matici $\mathbf{P}$, tedy inverzní matici k matici $\mathbf{A}$.

Pozorný čtenář by měl v tuto chvíli namítnout: proč je $\mathbf{P}$ inverzní matice k $\mathbf{A}$, když víme pouze, že $\mathbf{P} \cdot \mathbf{A} = \mathbf{E}$, ale nevíme, jestli $\mathbf{A} \cdot \mathbf{P} = \mathbf{E}$? Tento vzorec ale z existence inverzní matice pro regulární matici $\mathbf{A}$ plyne z prvního. Nechť $\mathbf{A}^{-1}$ je inverzní matice k matici $\mathbf{A}$ a nechť platí $\mathbf{P} \cdot \mathbf{A} = \mathbf{E}$. Vynásobíme nyní obě strany rovnice maticí $\mathbf{A}^{-1}$ zprava:

$$(\mathbf{P} \cdot \mathbf{A}) \cdot \mathbf{A}^{-1} = \mathbf{E} \cdot \mathbf{A}^{-1}, \quad \text{tj.} \quad \mathbf{P} \cdot (\mathbf{A} \cdot \mathbf{A}^{-1}) = \mathbf{A}^{-1}, \quad \text{tj.} \quad \mathbf{P} = \mathbf{A}^{-1}.$$

3.57. Poznámka. Všimněme si, že metoda hledání inverzních matic, popsaná v příkladu 3.53 a dokázaná ve větě 3.56 nám mimochodem umožní odpovědět i na otázku, zda vůbec inverzní matice k dané matici $\mathbf{A}$ existuje. Pokud zapíšeme $(\mathbf{A}|\mathbf{E})$ a na konci přímého chodu Gaussovy eliminační metody zjistíme, že v poli vlevo od svislé čáry máme nulový řádek, pak podle věty 3.17 víme, že $\mathbf{A}$ je singulární. Věta 3.50 nám říká, že inverzní matice neexistuje, takže nemá smysl dál počítat.

3.58. Poznámka. Kdybychom napsali jednotkovou matici pod matici $\mathbf{A}$ a aplikovali na sloupce této „dvojmatice" sloupcové úpravy podle Gaussovy eliminační metody a získali nakonec v horní části matici $\mathbf{E}$, pak je ve spodní části matice inverzní. Při důkazu tohoto tvrzení bychom postupovali analogicky jako při řádkové metodě, jen maticemi $\mathbf{P}_i$, které „emulují" sloupcové úpravy, bychom násobili matici $\mathbf{A}$ zprava a nikoli zleva.

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

3.59. Příklad. Najdeme matici $\mathbf{X}$ takovou, aby byla splněna rovnice

$$\mathbf{A}\cdot\mathbf{X}-\mathbf{X}+4\,\mathbf{A}=\mathbf{O},$$

kde $\mathbf{A}$ je matice typu $(3,3)$ z příkladu 3.53 a $\mathbf{O}$ je nulová matice stejného typu.

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

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

Pokud existuje matice $(\mathbf{A}-\mathbf{E})^{-1}$, pak po pronásobení obou stran rovnice touto maticí *zleva* dostáváme

$$\mathbf{X}=(\mathbf{A}-\mathbf{E})^{-1}\cdot(-4\,\mathbf{A})=-4\,(\mathbf{A}-\mathbf{E})^{-1}\cdot\mathbf{A}.$$

Je tedy potřeba najít inverzní matici k matici $\mathbf{A}-\mathbf{E}$ (například metodou popsanou v příkladu 3.53). Nalezenou inverzní matici vynásobíme čtyřmi a nakonec provedeme maticové násobení $4\,(\mathbf{A}-\mathbf{E})^{-1}\cdot\mathbf{A}$ podle definice. Níže uvádíme jednotlivé mezivýpočty:

$$\mathbf{A}-\mathbf{E}=\begin{pmatrix}0&2&3\\-1&-1&1\\2&2&0\end{pmatrix},\quad(\mathbf{A}-\mathbf{E})^{-1}=\begin{pmatrix}-\frac12&\frac32&\frac54\\\frac12&-\frac32&-\frac34\\0&1&\frac12\end{pmatrix},\quad4\,(\mathbf{A}-\mathbf{E})^{-1}=\begin{pmatrix}-2&6&5\\2&-6&-3\\0&4&2\end{pmatrix},$$

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

3.60. Věta. Nechť $\mathbf{A}$ je libovolná matice (ne nutně čtvercová) a $\mathbf{P}$, $\mathbf{Q}$ jsou regulární matice takové, že je definováno násobení $\mathbf{P}\cdot\mathbf{A}$ a $\mathbf{A}\cdot\mathbf{Q}$. Pak $\operatorname{hod}\mathbf{A}=\operatorname{hod}(\mathbf{P}\cdot\mathbf{A})=\operatorname{hod}(\mathbf{A}\cdot\mathbf{Q})$. Jinými slovy: násobení regulární maticí nemění hodnost. *Hodnost součinu matic*

Důkaz. Označme $\mathbf{B}=\mathbf{P}\cdot\mathbf{A}$. Sestavíme matici $(\mathbf{A}|\mathbf{E})$ a budeme ji eliminovat, abychom vpravo od čáry získali matici $\mathbf{P}$, tj. podle věty 3.55 dostáváme $(\mathbf{A}|\mathbf{E})\sim(\mathbf{P}\cdot\mathbf{A}\,|\,\mathbf{P}\cdot\mathbf{E})=(\mathbf{B}|\mathbf{P})$. Protože $\mathbf{P}$ je regulární, takovou eliminaci lze určitě provést. Kdo tomu nevěří, může eliminovat „pozpátku" od matice $\mathbf{P}$ k matici $\mathbf{E}$ a použít pak větu 3.10. Proveďme nakonec tutéž eliminaci znovu, jen s maticemi vlevo od svislé čáry: $\mathbf{A}\sim\mathbf{B}$. Protože Gaussova eliminace zachovává hodnost (věta 3.17), je $\operatorname{hod}\mathbf{A}=\operatorname{hod}\mathbf{B}=\operatorname{hod}(\mathbf{P}\cdot\mathbf{A})$.

K důkazu $\operatorname{hod}\mathbf{A}=\operatorname{hod}(\mathbf{A}\cdot\mathbf{Q})$ stačí podle (5) věty 3.38 přejít k transponovaným maticím a použít předchozí výsledek společně s větou 3.31: $\operatorname{hod}(\mathbf{A}\cdot\mathbf{Q})=\operatorname{hod}(\mathbf{A}\cdot\mathbf{Q})^T=\operatorname{hod}(\mathbf{Q}^T\cdot\mathbf{A}^T)=\operatorname{hod}\mathbf{A}^T=\operatorname{hod}\mathbf{A}$.

3.61. Věta. Je-li $\mathbf{A}\cdot\mathbf{B}$ definováno, pak $\operatorname{hod}(\mathbf{A}\cdot\mathbf{B})\le\min(\operatorname{hod}\mathbf{A},\operatorname{hod}\mathbf{B})$.

Důkaz. Je-li $h=\operatorname{hod}\mathbf{A}$, pak lze provést eliminaci $\mathbf{A}\sim\mathbf{C}$ takovou, že matice $\mathbf{C}$ má prvních h řádků nenulových a zbylé řádky nulové. Podle věty 3.55 existuje regulární $\mathbf{P}$ taková, že $\mathbf{A}=\mathbf{P}\cdot\mathbf{C}$. Na levé straně dokazované nerovnosti tedy máme $\operatorname{hod}(\mathbf{A}\cdot\mathbf{B})=\operatorname{hod}(\mathbf{P}\cdot\mathbf{C}\cdot\mathbf{B})=\operatorname{hod}(\mathbf{C}\cdot\mathbf{B})$. V poslední úpravě jsme použili větu 3.60. Nyní je potřeba si uvědomit, že díky nulovým řádkům matice $\mathbf{C}$ má matice $\mathbf{C}\cdot\mathbf{B}$ pod h-tým řádkem všechny ostatní řádky nulové. Takže $\operatorname{hod}(\mathbf{C}\cdot\mathbf{B})\le h=\operatorname{hod}\mathbf{A}$. Dostáváme výsledek $\operatorname{hod}(\mathbf{A}\cdot\mathbf{B})\le\operatorname{hod}\mathbf{A}$. Přejdeme nyní k maticím transponovaným $(\mathbf{A}\cdot\mathbf{B})^T=\mathbf{B}^T\cdot\mathbf{A}^T$. Znovu použijeme právě dokázaný výsledek a větu 3.31: $\operatorname{hod}(\mathbf{A}\cdot\mathbf{B})=\operatorname{hod}(\mathbf{A}\cdot\mathbf{B})^T=\operatorname{hod}(\mathbf{B}^T\cdot\mathbf{A}^T)\le\operatorname{hod}\mathbf{B}^T=\operatorname{hod}\mathbf{B}$. Protože $\operatorname{hod}(\mathbf{A}\cdot\mathbf{B})$ je menší nebo rovna $\operatorname{hod}\mathbf{A}$ i $\operatorname{hod}\mathbf{B}$, musí být menší nebo rovna minimu těchto hodnot.

4. Determinant

Determinant je číslo, které jistým způsobem charakterizuje čtvercovou matici. Toto číslo má mnoho důležitých významů, se kterými se setkáme nejen v lineární algebře, ale i v jiných matematických disciplínách. Determinant se podle definice počítá z prvků matice poměrně komplikovaným způsobem. Než budeme schopni tuto definici formulovat, musíme si něco říci o permutacích. Na tomto pojmu je totiž definice determinantu založena.

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

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

4.3. Věta. Počet různých permutací n prvků je roven číslu $n!$.

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

Matematickou indukcí dokazujeme tvrzení, které má platit pro všechna $n \in \mathbf{N}$. Postupujeme ve dvou krocích. Nejprve dokážeme toto tvrzení pro $n = 1$. Pak dokážeme tzv. indukční krok, který je formulován ve tvaru implikace: „jestliže tvrzení platí pro n, pak platí pro $n + 1$“. Obhájíme-li platnost této implikace, máme dokázáno tvrzení pro všechna $n \in \mathbf{N}$. Vysvětlíme si, proč. V prvním kroku jsme dokázali, že tvrzení platí pro $n = 1$. Uplatníme nyní indukční krok ve tvaru „jestliže tvrzení platí pro $n = 1$, pak platí pro $n = 2$“. Tím máme zaručeno, že tvrzení platí pro $n = 2$. Zopakujeme indukční krok, tentokrát ve tvaru „jestliže tvrzení platí pro $n = 2$, pak platí pro $n = 3$“. To dokazuje platnost tvrzení pro $n = 3$. Opakovaným uplatněním indukčního kroku jsme schopni doložit platnost tvrzení pro libovolně velké n.

Tvrzení naší věty je: „počet různých permutací n prvků je roven číslu $n!$“. Dokážeme v prvním kroku pro $n = 1$, tj. „počet různých permutací jednoho prvku je roven číslu $1! = 1$“. O tom ale asi nikdo nepochybuje, nelze totiž vytvořit nic jiného než permutaci (1).

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

4.4. Příklad. Uvedeme si všechny permutace tří prvků. Podle věty 4.3 je jejich počet roven šesti. Hledané permutace jsou:

$$(1, 2, 3), \quad (1, 3, 2), \quad (2, 1, 3), \quad (2, 3, 1), \quad (3, 1, 2), \quad (3, 2, 1).$$

Zkusíme ještě zapsat všechny permutace čtyř prvků. Je jich 24.

$$\begin{array}{llllllll}
(1,2,3,4), & (1,2,4,3), & (1,3,2,4), & (1,3,4,2), & (1,4,2,3), & (1,4,3,2), & (2,1,3,4), & (2,1,4,3), \\
(2,3,1,4), & (2,3,4,1), & (2,4,1,3), & (2,4,3,1), & (3,2,1,4), & (3,2,4,1), & (3,1,2,4), & (3,1,4,2), \\
(3,4,2,1), & (3,4,1,2), & (4,2,3,1), & (4,2,1,3), & (4,3,2,1), & (4,3,1,2), & (4,1,2,3), & (4,1,3,2).
\end{array}$$

Kdybychom chtěli zapsat všechny permutace 50 prvků, po použití věty 4.3 bychom si to rychle rozmysleli. Těch permutací totiž je přibližně $3 \cdot 10^{64}$. Kdyby se nám na jeden řádek vešla jedna permutace a na stránku 60 řádků, spotřebovali bychom $5 \cdot 10^{62}$ stránek. Při oboustranném tisku váží 500 stránek asi jeden kilogram, takže bychom spotřebovali 10^{57} tun papíru. Kdyby tisk jedné stránky trval vteřinu, strávili bychom u tiskárny zhruba 10^{55} let. Jistě uznáte, že to daleko přesahuje veškeré lidské možnosti.

4.5. Definice. Nechť $(i_1, i_2, \ldots, i_n)$ je permutace n prvků. *Inverze* této permutace je taková dvojice (i_k, i_l), pro které platí $i_k > i_l$, a přitom $k < l$.

4.6. Příklad. Permutace $(1, 2, 3)$ nemá žádnou inverzi. Permutace $(1, 3, 2)$ má jednu inverzi, totiž dvojici $(3, 2)$, pro kterou platí $3 > 2$. Jednotlivé inverze jsou na následujících permutacích vyznačeny obloučkem

$$(1, 2, 3), \quad (1, 3, 2), \quad (2, 1, 3), \quad (2, 3, 1), \quad (3, 1, 2), \quad (3, 2, 1).$$

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

Znaménko permutace

4.7. Definice. Pro každou permutaci $\pi = (i_1, \ldots, i_n)$ definujeme *znaménko permutace* $\operatorname{sgn} \pi$ takto:

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

4.8. Příklad. Permutace z příkladu 4.6 mají tato znaménka:

$$\begin{aligned} &\operatorname{sgn}(1, 2, 3) = +1, \quad \operatorname{sgn}(1, 3, 2) = -1, \quad \operatorname{sgn}(2, 1, 3) = -1, \\ &\operatorname{sgn}(2, 3, 1) = +1, \quad \operatorname{sgn}(3, 1, 2) = +1, \quad \operatorname{sgn}(3, 2, 1) = -1. \end{aligned}$$

Jako cvičení si rozmyslete, jak vypadají znaménka všech permutací čtyř prvků.

4.9. Věta. Prohození jediné dvojice prvků v permutaci způsobí změnu jejího znaménka.

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

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

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

$$\pi = (\ldots, x, \ldots, a, \ldots, z, \ldots, b, \ldots, y, \ldots), \quad \pi_1 = (\ldots, x, \ldots, b, \ldots, z, \ldots, a, \ldots, y, \ldots).$$

Nemusejí v každém případě všechny tyto prvky existovat. Další rozbor tedy provedeme jen tehdy, pokud příslušný prvek existuje. Zabývejme se nejprve prvky x a y. Případné inverze mezi prvky (x, a), (x, b), (a, y) a (b, y) zůstanou po prohození prvků a, b v nezměněném stavu. Zajímavý je tedy jen prvek z.

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

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

4.11. Poznámka. Existuje několik možností, jak si představit inverzní permutaci k dané permutaci.

(1) Je-li v permutaci π na x-tém místě prvek y, pak v permutaci π^{-1} musí být na y-tém místě prvek x.

(2) Zapišme pod sebe permutaci π a permutaci $(1, 2, \ldots, n)$ takto:

$$\begin{pmatrix} i_1 & i_2 & i_3 & \ldots & i_n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}$$

a zaměnme pořadí sloupců této matice tak, abychom v prvním řádku měli vzestupně čísla $(1, 2, 3, \ldots, n)$. Pak ve spodním řádku je zapsána inverzní permutace k permutaci π. Uvažujme kupříkladu permutaci $(3, 4, 2, 6, 1, 5)$ a pišme:

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

Je tedy $(3, 4, 2, 6, 1, 5)^{-1} = (5, 3, 1, 2, 6, 4)$.

(3) Představme si šachovnici o rozměru $n \times n$ a rozestavme na ní n šachových věží tak, aby se vzájemně neohrožovaly. Takových rozestavení může být více a každé rozestavení můžeme popsat jednoznačně jako permutaci. V každém řádku i sloupci totiž stojí jediná věž a my můžeme číst rozestavení po řádcích takto: do první složky permutace napíšeme číslo sloupce, na kterém stojí věž z prvního řádku, do druhé složky číslo sloupce, na které stojí věž z druhého řádku atd. Dostáváme tak permutaci π. Pokud nyní čteme totéž rozestavení po sloupcích, tj. do první složky permutace napíšeme číslo řádku věže z prvního sloupce, do druhé složky číslo řádku věže z druhého sloupce atd., dostáváme permutaci π^{-1}.

(4) Na permutaci n prvků můžeme pohlížet jako na zobrazení $\pi\colon M \to M$, kde $M = \{1, 2, \ldots, n\}$. Pak inverzní permutace odpovídá inverznímu zobrazení. Zná-li už čtenář pojem skládání funkcí $(f \circ g)$, pak může ověřit, že platí $\pi \circ \pi^{-1} = (1, 2, 3, \ldots, n)$.

4.12. Věta. Nechť π je permutace n prvků. Pak π^{-1} má stejný počet inverzí, jako π.

Důkaz. Pro názornost si představíme inverzní permutaci způsobem (2) z poznámky 4.11. Zaměřme se na dva sloupce uvedené dvouřádkové matice před prohozením 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 $x < y$, tj. (x, y) netvoří inverzi v permutaci π, zůstanou po prohození sloupců tyto dva sloupce za sebou ve stejném pořadí. Takže se nová inverze v permutaci π^{-1} nevytvoří. Pokud ale $x > y$, tj. (x, y) tvoří inverzi v permutaci π, pak po prohození sloupců budou tyto dva sloupce v opačném pořadí. Dvojice prvků (b, a) tedy bude tvořit inverzi v permutaci π^{-1}.

4.13. Věta. Permutace π a π^{-1} mají vždy stejná znaménka.

Důkaz. Věta je přímým důsledkem věty 4.12.

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

4.15. Definice. Nechť $\mathbf{A} = (a_{i,j})$ je čtvercová matice typu (n, n). Číslo *Definice determinantu*

$$\sum_{\pi=(i_1,i_2,\ldots,i_n)} \operatorname{sgn} \pi \cdot a_{1,i_1}\, a_{2,i_2} \cdots a_{n,i_n} \tag{4.1}$$

nazýváme *determinantem matice* $\mathbf{A}$ a značíme je $\det \mathbf{A}$. V uvedeném vzorci se sčítá přes všechny permutace n prvků, tj. jedná se podle věty 4.3 o $n!$ sčítanců.

4.16. Poznámka. Je možné, že vzorec z definice 4.15 je pro některé čtenáře málo srozumitelný. Pokusíme se jej proto v této poznámce trochu vysvětlit a zlidštit.

Představme si čtvercovou matici jako šachovnici rozměru $n \times n$ a pokusme se na ni rozmístit n šachových věží tak, aby se vzájemně neohrožovaly. Podle poznámky 4.11, odst. (3) je možné každé takové rozmístění popsat jednou permutací (pozice věží čteme po řádcích). Podle věty 4.3 vidíme, že existuje $n!$ různých permutací, tedy existuje $n!$ různých řešení této šachové úlohy. Pokusme se pro každé řešení této úlohy zapsat odpovídající permutaci, zjistit znaménko této permutace, nadzvednout věžičky a zapsat si hodnoty prvků, na kterých ty figurky stojí, vynásobit tyto hodnoty mezi sebou a výsledek ještě násobit znaménkem permutace. Pak si tento výsledek uložíme do paměti. Až projdeme všech $n!$ možností rozmístění věží, získáme v paměti $n!$ sčítanců a ty sečteme. Výsledkem je determinant matice.

4.17. Příklad. Hledejme determinant matice typu $(3,3)$ 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 4.15 budeme sčítat přes všechny permutace tří prvků. Těch je podle věty 4.3 $3! = 6$. Zapíšeme všechny tyto permutace, jejich znaménka a odpovídající rozmístění „šachových věží“.

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

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

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

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

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

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

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

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

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

4.18. Příklad. Podobně, jako v předchozím příkladě, odvodíme vzorec pro výpočet determinantu matice typu $(2,2)$.

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

$$\det \mathbf{A} = a_{1,1} \cdot a_{2,2} - a_{1,2} \cdot a_{2,1}.$$

Pro úplnost uvedeme ještě hodnotu determinantu matice $\mathbf{A} = (a_{1,1})$ typu $(1,1)$. Zřejmě je $\det \mathbf{A} = a_{1,1}$.

4.19. Definice. Nechť $\mathbf{A} = (a_{i,j})$ je matice typu (n,n). *Hlavní diagonála matice* $\mathbf{A}$ je skupina jejích prvků $a_{1,1}, a_{2,2}, \ldots, a_{n,n}$. *Vedlejší diagonála matice* $\mathbf{A}$ zahrnuje prvky $a_{1,n}, a_{2,n-1}, \ldots, a_{n,1}$. *Prvek pod hlavní diagonálou* je každý prvek $a_{i,j}$, pro který platí $i > j$. *Prvek nad hlavní diagonálou* je každý prvek $a_{i,j}$, pro který platí $i < j$.

4.20. Příklad. Nechť matice $\mathbf{A}$ typu (n,n) má pod hlavní diagonálou jen nulové prvky. Matice tedy názorně vypadá takto:

$$\mathbf{A} = \begin{pmatrix} a_{1,1}, & a_{1,2}, & \ldots, & a_{1,n-1}, & a_{1,n} \\ 0, & a_{2,2}, & \ldots, & a_{2,n-1}, & a_{2,n} \\ 0, & 0, & \ldots, & a_{3,n-1}, & a_{3,n} \\ & & \vdots & & \\ 0, & 0, & \ldots, & 0, & a_{n,n} \end{pmatrix}. \tag{4.2}$$

Zkusíme spočítat $\det \mathbf{A}$.

V definici determinantu 4.15 se pracuje se součtem součinů $\operatorname{sgn} \pi \cdot a_{1,i_1} \cdot a_{2,i_2} \cdots a_{n,i_n}$. Pokud aspoň jeden z těchto činitelů je nulový, je nulový celý součin. V celkovém součtu nás zajímají jen nenulové součiny. Prozkoumejme, které to jsou. Z posledního řádku musíme vzít jen prvek $a_{n,n}$, protože všechny ostatní prvky v posledním řádku jsou nulové. Z předposledního řádku můžeme vzít jen prvek $a_{n-1,n-1}$, protože ostatní jsou nulové. Prvek $a_{n-1,n}$ nelze do součinu zahrnout, protože z posledního sloupce už v součinu máme prvek $a_{n,n}$ (věže by se vzájemně ohrožovaly). Analogickou úvahou zahrneme do součinu prvky $a_{n-2,n-2}, \ldots, a_{2,2}, a_{1,1}$. Není tedy jiná možnost nenulového součinu, než součin $a_{1,1} \cdot a_{2,2} \cdots a_{n,n}$. Ten odpovídá permutaci $(1,2,\ldots,n)$, která nemá žádnou inverzi a její znaménko je tedy $+1$. Ostatní sčítanci z definice determinantu jsou nuloví. Proto $\det \mathbf{A} = a_{1,1} \cdot a_{2,2} \cdot a_{3,3} \cdots a_{n,n}$.

4.21. Věta. Základní vlastnosti determinantu. *Základní vlastnosti*

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

(V2) Jestliže matice $\mathbf{A}$ má dva stejné řádky, pak $\det \mathbf{A} = 0$.

V dalších vlastnostech (V3) až (V5) označujeme symbolem $\begin{pmatrix} \vdots \\ \boldsymbol{a}_i \\ \vdots \end{pmatrix}$ matice, které se liší pouze v i-tém řádku, zde označeném $\boldsymbol{a}_i$. V řádcích, které jsou vyznačeny tečkami, se jednotlivé matice shodují.

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

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

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

Důkaz. (V1) Součin $a_{1,i_1} \cdots a_{n,i_n}$ odpovídá ve vzorci pro výpočet $\det \mathbf{A}$ permutaci $\pi = (i_1, i_2, \ldots, i_n)$. Tentýž součin najdeme i ve vzorci pro výpočet $\det \mathbf{B}$, pouze bude odpovídat permutaci π', která vznikne z permutace π přehozením dvou prvků. To podle věty 4.9 znamená, že $\operatorname{sgn} \pi' = -\operatorname{sgn} \pi$. V každém z $n!$ sčítanců pro výpočet $\det \mathbf{B}$ tedy máme opačné znaménko, než ve sčítancích pro výpočet $\det \mathbf{A}$. Musí tedy být $\det \mathbf{B} = -\det \mathbf{A}$.

(V2) Prohodíme-li v matici $\mathbf{A}$ mezi sebou dva stejné řádky, dostáváme zase matici $\mathbf{A}$. Podle (V1) pro tuto matici platí $\det \mathbf{A} = -\det \mathbf{A}$, což nemůže být splněno jinak, než že $\det \mathbf{A} = 0$.

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

$$\text{(V3)} \quad \sum \operatorname{sgn} \pi\, a_{1,j_1}\, a_{2,j_2} \cdots (\alpha\, a_{i,j_i})\, a_{i+1,j_{i+1}} \cdots a_{n,j_n} = \alpha \sum \operatorname{sgn} \pi\, a_{1,j_1}\, a_{2,j_2} \cdots a_{i,j_i}\, a_{i+1,j_{i+1}} \cdots a_{n,j_n}.$$

$$\text{(V4)} \quad \sum \operatorname{sgn} \pi\, a_{1,j_1}\, a_{2,j_2} \cdots (a_{i,j_i} + b_{i,j_i})\, a_{i+1,j_{i+1}} \cdots a_{n,j_n} =$$

$$= \sum \operatorname{sgn} \pi\, a_{1,j_1}\, a_{2,j_2} \cdots a_{i,j_i}\, a_{i+1,j_{i+1}} \cdots a_{n,j_n} + \sum \operatorname{sgn} \pi\, a_{1,j_1}\, a_{2,j_2} \cdots b_{i,j_i}\, a_{i+1,j_{i+1}} \cdots a_{n,j_n}.$$

(V5) dokážeme použitím právě dokázaných vlastností:

$$\det\begin{pmatrix}\vdots\\ \boldsymbol{a}_j\\ \vdots\\ \boldsymbol{a}_i+\alpha\,\boldsymbol{a}_j\\ \vdots\end{pmatrix} \overset{\text{(V4)}}{=} \det\begin{pmatrix}\vdots\\ \boldsymbol{a}_j\\ \vdots\\ \boldsymbol{a}_i\\ \vdots\end{pmatrix} + \det\begin{pmatrix}\vdots\\ \boldsymbol{a}_j\\ \vdots\\ \alpha\,\boldsymbol{a}_j\\ \vdots\end{pmatrix} \overset{\text{(V3)}}{=} \det\begin{pmatrix}\vdots\\ \boldsymbol{a}_j\\ \vdots\\ \boldsymbol{a}_i\\ \vdots\end{pmatrix} + \alpha\det\begin{pmatrix}\vdots\\ \boldsymbol{a}_j\\ \vdots\\ \boldsymbol{a}_j\\ \vdots\end{pmatrix} \overset{\text{(V2)}}{=} \det\begin{pmatrix}\vdots\\ \boldsymbol{a}_j\\ \vdots\\ \boldsymbol{a}_i\\ \vdots\end{pmatrix}.$$

Metoda počítání determinantu

4.22. Poznámka. Vlastnosti (V1), (V3) a (V5) nám ukazují, jak se změní determinant, změníme-li matici pomocí Gaussovy eliminační metody. Prohození řádků změní znaménko, vynásobení řádku nenulovým číslem α způsobí, že se determinant α-krát zvětší a konečně přičtení α-násobku jiného řádku ke zvolenému řádku nezmění hodnotu determinantu. Jsme tedy schopni upravovat matice Gaussovou eliminační metodou, a přitom si poznamenávat, jak se mění determinant. Tím můžeme převést matici na tvar (4.2). O této matici víme, že má determinant roven součinu prvků na hlavní diagonále.

Uvědomme si, že tato metoda dává výraznou úsporu času a výpočetních prostředků při počítání determinantů. Představme si, že počítáme determinant matice typu (n, n). Při Gaussově eliminační metodě potřebujeme zhruba n operací na výrobu jednoho nulového prvku. Těch nul potřebujeme vytvořit zhruba $n^2/2$, takže k výpočtu determinantu nám stačí $n^3/2$ operací. Pro matici typu $(50, 50)$ to je zhruba 62 500 operací. Pokud bychom chtěli počítat determinant stejně velké matice přímo z definice, potřebovali bychom na to $50 \cdot 3 \cdot 10^{64}$ operací (viz komentář v příkladu 4.4). Není v silách žádné výpočetní techniky spočítat to v rozumném čase.

4.23. Příklad. Právě popsanou metodou spočítáme determinant matice

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

V literatuře se pro $\det\mathbf{A}$ často používá značení $|\mathbf{A}|$. Níže tedy zapisujeme prvky jednotlivých matic mezi svislé čáry a tím dáváme na jevo, že počítáme determinant.

$$\begin{vmatrix}1&2&4&-1\\2&1&2&2\\1&3&1&2\\2&1&2&1\end{vmatrix} \overset{(1)}{=} \begin{vmatrix}1&2&4&-1\\0&-3&-6&4\\0&1&-3&3\\0&-3&-6&3\end{vmatrix} \overset{(2)}{=} -\begin{vmatrix}1&2&4&-1\\0&1&-3&3\\0&-3&-6&4\\0&-3&-6&3\end{vmatrix} \overset{(3)}{=} -\begin{vmatrix}1&2&4&-1\\0&1&-3&3\\0&0&-15&13\\0&0&-15&12\end{vmatrix} \overset{(4)}{=}$$

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

V kroku (1) jsme první řádek násobili -2 a přičítali k druhému, pak jsme první řádek násobili -1 a přičítali k třetímu a nakonec jsme první řádek násobili -2 a přičítali ke čtvrtému. Tyto operace podle (V5) nemění hodnotu determinantu. V kroku (2) jsme prohodili druhý řádek se třetím, což podle (V1) změní znaménko determinantu. Napsali jsme toto znaménko před determinant modifikované matice. V kroku (3) jsme druhý řádek násobili třemi a přičetli ke třetímu a čtvrtému. To podle (V5) nemění hodnotu determinantu. Konečně v kroku (4) jsme třetí řádek násobili -1 a přičetli ke čtvrtému. Tím dostáváme matici tvaru (4.2) z příkladu 4.20, o které víme, že má determinant roven součinu prvků na diagonále.

Upozorňujeme na častou začátečnickou chybu při počítání determinantů. V Gaussově eliminační metodě se většinou neklade důraz na to, který řádek od kterého odečítáme, protože výsledný řádek můžeme kdykoli později násobit číslem -1. Při počítání determinantů to ale jedno není. Například v kroku (1) jsme od druhého řádku odečítali dvojnásobek prvního a výsledek psali na druhý řádek. Kdybychom od dvojnásobku prvního řádku odečítali druhý a výsledek psali do druhého řádku, dopustili bychom se chyby, která nám změní znaménko determinantu. Mnemotechnická pomůcka: píšeme-li výsledek součtu na i-tý řádek, pak i-tý řádek původní matice nesmí být v součtu násoben žádnou konstantou. Ostatní řádky mohou být násobeny libovolnou konstantou a přičítány k tomuto řádku. Je třeba si tedy uvědomit, že „přičtení násobku řádku $\boldsymbol{a}$ k řádku $\boldsymbol{b}$“ (korektní krok) není totéž, jako „přičtení řádku $\boldsymbol{a}$ k násobku řádku $\boldsymbol{b}$“ (nekorektní krok).

4.24. Příklad. Jednotková matice má determinant roven jedné. Jednotková matice je totiž tvaru (4.2), takže stačí pronásobit prvky na diagonále.

4.25. Příklad. Nechť $\mathbf{A}$ je matice typu (n, n), která má prvky na vedlejší diagonále rovny jedné a ostatní prvky jsou nulové. Spočítáme její determinant.

Prohodíme první řádek s posledním, druhý s předposledním atd. až se dostaneme k prostřednímu řádku. Pro liché n necháváme prostřední řádek na místě, pro sudé n prohodíme naposled mezi sebou řádky $n/2$ a $n/2 + 1$. V obou případech jsme udělali $[n/2]$ prohození (symbolem $[x]$ zde značíme celou část z x). Matici $\mathbf{A}$ jsme těmito úpravami převedli na jednotkovou matici $\mathbf{E}$. Podle předchozího příkladu je $\det \mathbf{E} = 1$, takže podle vlastnosti (V1) z věty 4.21 je $\det \mathbf{A} = (-1)^{[n/2]} \det \mathbf{E} = (-1)^{[n/2]}$.

4.26. Příklad. Nechť $\mathbf{A}$ je matice typu (n, n), která má nad vedlejší diagonálou nulové prvky. Spočítáme její determinant.

Prohazováním řádků, stejně jako v předchozím příkladě, převedeme matici na tvar (4.2). Prvky z vedlejší diagonály se při těchto úpravách přestěhují na hlavní diagonálu. Determinant takto upravené matice je podle příkladu 4.20 roven součinu prvků na diagonále, takže máme $\det \mathbf{A} = (-1)^{[n/2]} a_{1,n}\, a_{2,n-1} \cdots a_{n,1}$.

4.27. Věta. Čtvercová matice $\mathbf{A}$ je regulární právě tehdy, když $\det \mathbf{A} \neq 0$.

Důkaz. Všimneme si nejprve, že Gaussova eliminační metoda realizovaná kroky (V1), (V3) a (V5) podle předchozí věty 4.21 nemění „nulovost" determinantu. Přesněji, je-li $\mathbf{A} \sim \mathbf{B}$, pak $\det \mathbf{A} \neq 0$ právě tehdy když $\det \mathbf{B} \neq 0$.

Je-li matice $\mathbf{A}$ regulární ($\operatorname{hod} \mathbf{A} = n$), pak po úpravě Gaussovou eliminační metodou na matici $\mathbf{B}$ tvaru (4.2) musejí být všechny prvky na diagonále nenulové, protože podle věty 3.17 je také $\operatorname{hod} \mathbf{B} = n$. To znamená, že $\det \mathbf{B} \neq 0$ a tedy i $\det \mathbf{A} \neq 0$.

Je-li matice $\mathbf{A}$ singulární ($\operatorname{hod} \mathbf{A} < n$), pak po úpravě Gaussovou eliminační metodou na matici $\mathbf{B}$ tvaru (4.2) bude existovat aspoň jeden řádek v matici $\mathbf{B}$ celý nulový. Nulový je tedy i diagonální prvek, takže $\det \mathbf{B} = 0$. Podle předchozího nutně musí být $\det \mathbf{A} = 0$.

4.28. Věta. Nechť $\mathbf{A}$ je čtvercová matice. Pak $\det \mathbf{A} = \det \mathbf{A}^T$.

Důkaz. Součinu $a_{1,i_1}\, a_{2,i_2} \cdots a_{n,i_n}$ ze vzorce (4.1) pro $\det \mathbf{A}$ odpovídá permutace $\pi = (i_1, i_2, \ldots, i_n)$. Uspořádáme činitele tohoto součinu podle velikosti druhého indexu a dostaneme $a_{j_1,1}\, a_{j_2,2} \cdots a_{j_n,n}$, kde pro permutaci $\pi_1 = (j_1, j_2, \ldots, j_n)$ platí $\pi_1 = \pi^{-1}$. Právě takové součiny se objevují ve vzorci pro $\det \mathbf{A}^T$. Vidíme tedy, že oba vzorce $\det \mathbf{A}$ i $\det \mathbf{A}^T$ obsahují sumu stejných součinů, pouze permutace odpovídajících součinů je v prvním případě π a v druhém π^{-1}. Tyto permutace mají podle věty 4.12 stejný počet inverzí, takže i stejné znaménko. Musí tedy být $\det \mathbf{A} = \det \mathbf{A}^T$.

4.29. Poznámka. Z právě dokázané věty plyne, že vlastnosti vyjmenované ve větě 4.21 platí nejen pro řádky matice, ale též pro sloupce. Při počítání determinantu podle metody popsané v poznámce 4.22 můžeme tedy svobodně přecházet od řádkových úprav ke sloupcovým a zpět, protože vlastnosti (V1), (V3) a (V5) věty 4.21 platí nejen pro řádky, ale i pro sloupce (tzv. řádkově-sloupcová dualita).

Rozvoj determinantu

4.30. Věta (o rozvoji determinantu podle r-tého řádku). Nechť $\mathbf{A} = (a_{r,s})$ je čtvercová matice typu (n, n) a $\mathbf{A}_{i,j}$ jsou matice typu $(n-1, n-1)$, které vzniknou z matice $\mathbf{A}$ vynecháním i-tého řádku a j-tého sloupce. Pak pro každé $r \in \{1, \ldots, n\}$ platí

$$a_{r,1}\, (-1)^{r+1} \det \mathbf{A}_{r,1} + a_{r,2}\, (-1)^{r+2} \det \mathbf{A}_{r,2} + \cdots + a_{r,n}\, (-1)^{r+n} \det \mathbf{A}_{r,n} = \det \mathbf{A}. \tag{4.3}$$

Je-li dále $t \in \{1, \ldots, n\}$, $t \neq r$, pak platí

$$a_{r,1}\, (-1)^{t+1} \det \mathbf{A}_{t,1} + a_{r,2}\, (-1)^{t+2} \det \mathbf{A}_{t,2} + \cdots + a_{r,n}\, (-1)^{t+n} \det \mathbf{A}_{t,n} = 0. \tag{4.4}$$

Důkaz (pro hloubavé čtenáře). Podívejme se na vzorec (4.1) pro $\det \mathbf{A}$. Seskupíme v něm všechny sčítance, které obsahují prvek $a_{1,1}$ k sobě, dále seskupíme k sobě sčítance, které obsahují prvek $a_{1,2}$ a tak dále až po poslední skupinu, ve které se vyskytují sčítanci s prvkem $a_{1,n}$. Tyto prvky ze součtů vytkneme. Pro s-tou skupinu sčítanců tedy máme:

$$\sum_{\pi=(s,i_2,\ldots,i_n)} \operatorname{sgn} \pi \cdot a_{1,s}\, a_{2,i_2} \cdots a_{n,i_n} = a_{1,s} \left(\sum_{\pi=(s,i_2,\ldots,i_n)} \operatorname{sgn} \pi \cdot a_{2,i_2} \cdots a_{n,i_n} \right) = *$$

Z permutace $\pi = (s, i_2, \ldots, i_n)$ prvků množiny $M = \{1, 2, \ldots, n\}$ vytvořme permutaci $\pi' = (i_2, \ldots, i_n)$ prvků množiny $M \setminus \{s\}$ tak, že odebereme první prvek z permutace π. Nová permutace π' má o $s-1$ méně inverzí než permutace π. (Nakreslete si všechny inverze spojené s prvkem s.) Pro znaménka permutací tedy platí $\operatorname{sgn}\pi = (-1)^{s-1}\operatorname{sgn}\pi' = (-1)^{s+1}\operatorname{sgn}\pi'$. Pokračujme nyní dále v našem výpočtu:

$$* = a_{1,s}\,(-1)^{1+s}\left(\sum_{\pi'=(i_2,\ldots,i_n)} \operatorname{sgn}\pi' \cdot a_{2,i_2}\cdots a_{n,i_n}\right) = a_{1,s}\,(-1)^{1+s}\det \mathbf{A}_{1,s}.$$

Determinant $\mathbf{A}$ je součtem všech skupin sčítanců pro $s = 1, 2, \ldots, n$, což dokazuje vzorec (4.3) pro $r = 1$.

Nechť nyní $r \neq 1$. Prohodíme r-tý řádek matice $\mathbf{A}$ s předchozím, pak jej prohodíme s dalším předcházejícím řádkem, atd. až dostaneme původně r-tý řádek na první řádek modifikované matice $\mathbf{B}$. K tomu potřebujeme provést $r-1$ prohození, takže platí $\det\mathbf{B} = (-1)^{r-1}\det\mathbf{A}$. Provedeme rozvoj determinantu matice $\mathbf{B}$ podle prvního řádku ($\mathbf{B}_{1,s}$ je matice, která vznikne z matice $\mathbf{B}$ vynecháním prvního řádku a s-tého sloupce):

$$\det\mathbf{B} = a_{r,1}\,(-1)^{1+1}\det\mathbf{B}_{1,1} + a_{r,2}\,(-1)^{2+1}\det\mathbf{B}_{1,2} + \cdots + a_{r,n}\,(-1)^{1+n}\det\mathbf{B}_{1,n}.$$

Protože $\det\mathbf{A} = (-1)^{r-1}\det\mathbf{B}$ a protože $\mathbf{B}_{1,s} = \mathbf{A}_{r,s}$, máme vzorec (4.3) dokázán.

Uvažujme $t \neq r$ a nahraďme t-tý řádek v matici $\mathbf{A}$ řádkem r-tým. Novou matici označme $\mathbf{C}$. Má dva stejné řádky, takže je $\det\mathbf{C} = 0$. Rozvoj tohoto determinantu podle t-tého řádku odpovídá vzorci (4.4).

4.31. Poznámka. Vzhledem k platnosti věty 4.28 platí analogická věta o rozvoji determinantu podle s-tého sloupce. Zkuste si ji zformulovat jako cvičení.

4.32. Definice. Nechť $\mathbf{A}$ je čtvercová matice typu (n,n). *Doplněk matice* $\mathbf{A}$ *v pozici* (i,j) je číslo $D_{i,j}$, definované vzorcem: $D_{i,j} = (-1)^{i+j}\det\mathbf{A}_{i,j}$, kde $\mathbf{A}_{i,j}$ je matice typu $(n-1,n-1)$, která vznikne z matice $\mathbf{A}$ vynecháním i-tého řádku a j-tého sloupce.

4.33. Poznámka. Větu 4.30 lze při použití definice 4.32 a poznámky 4.31 přeformulovat. Nechť $\mathbf{A}$ je čtvercová matice typu (n,n) a $D_{i,j}$ jsou její doplňky. Nechť $r, s, t \in \{1, 2, \ldots, n\}$, $r \neq t$, $s \neq t$. Pak platí

$$\begin{aligned} \det\mathbf{A} &= a_{r,1}\,D_{r,1} + a_{r,2}\,D_{r,2} + \cdots + a_{r,n}\,D_{r,n}, &\quad 0 &= a_{r,1}\,D_{t,1} + a_{r,2}\,D_{t,2} + \cdots + a_{r,n}\,D_{t,n},\\ \det\mathbf{A} &= a_{1,s}\,D_{1,s} + a_{2,s}\,D_{2,s} + \cdots + a_{n,s}\,D_{n,s}, &\quad 0 &= a_{1,s}\,D_{1,t} + a_{2,s}\,D_{2,t} + \cdots + a_{n,s}\,D_{n,t}. \end{aligned}$$

4.34. Příklad. Uvažujme matici $\mathbf{A}$ z příkladu 4.23. Provedeme rozvoj determinantu $\mathbf{A}$ podle prvního řádku.

$$\det\mathbf{A} = 1\cdot(-1)^{1+1}\cdot\begin{vmatrix}1&2&2\\3&1&2\\1&2&1\end{vmatrix} + 2\cdot(-1)^{1+2}\cdot\begin{vmatrix}2&2&2\\1&1&2\\2&2&1\end{vmatrix} + 4\cdot(-1)^{1+3}\cdot\begin{vmatrix}2&1&2\\1&3&2\\2&1&1\end{vmatrix} - 1\cdot(-1)^{1+4}\cdot\begin{vmatrix}2&1&2\\1&3&1\\2&1&2\end{vmatrix} =$$
$$= 1\cdot 5 + 2\cdot 0 + 4\cdot(-5) - 1\cdot 0 = -15.$$

Vidíme, že jsme si při výpočtu moc nepomohli. Rozvoj determinantu podle řádku nebo sloupce matice typu (n,n) obecně vede na n determinantů matic, které mají o jediný řádek a sloupec méně. To není žádná výhra.

Kdybychom opakovaně prováděli rozvoj vzniklých determinantů podle řádku nebo sloupce, mohli bychom dojít až k maticím typu (1,1), u kterých je determinant přímo roven hodnotě prvku dané matice. Programátory může napadnout, že lze tedy větu o rozvoji determinantu využít při implementaci výpočtu determinantu rekurzivním algoritmem. Ovšem pozor! Tento algoritmus potřebuje zcela stejné množství operací, jako při výpočtu determinantu přímo z definice. Jak už jsme si uváděli, při matici typu $(50,50)$ se jedná zhruba o 10^{64} operací. Prakticky to znamená, že bychom se pravděpodobně výsledku nedočkali za celou dobu předpokládané existence naší sluneční soustavy a kdo ví, jestli by se dříve nezhroutil vesmír.

Můžete namítnout, k čemu že je metoda rozvoje determinantu dobrá? Pokud se v nějakém řádku nebo sloupci matice vyskytuje mnoho nul, můžeme zmenšit velikost matic, ze kterých počítáme determinant. Je-li na řádku nebo sloupci jediný nenulový prvek, dostáváme jedinou matici o jeden řádek a sloupec menší. V příkladu 4.23 jsme mohli například před provedením kroku (2) provést rozvoj determinantu podle prvního sloupce a dále pracovat jen s maticí typu (3, 3). Před krokem (4) jsme mohli znovu provést rozvoj determinantu podle prvního sloupce:

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

$$= - \begin{vmatrix} 1 & -3 & 3 \\ 0 & -15 & 13 \\ 0 & -15 & 12 \end{vmatrix} = -1 \cdot \begin{vmatrix} -15 & 13 \\ -15 & 12 \end{vmatrix} = 15 \cdot 12 - 15 \cdot 13 = -15.$$

Výhoda se projeví výrazněji, pokud například čísla v prvním řádku či sloupci jsou nesoudělná a je výhodnější začít vyrábět nuly v jiném řádku nebo sloupci. Eliminační metodou v něm vytvoříme nuly a pak provedeme podle tohoto řádku nebo sloupce rozvoj determinantu.

4.35. Věta (Laplaceova). Nechť $\mathbf{A}$, $\mathbf{B}$ jsou čtvercové matice. Pak $\det \mathbf{A} \det \mathbf{B} = \det(\mathbf{A} \cdot \mathbf{B})$.

Součin determinantů

Důkaz (pro hloubavé čtenáře). Uvědomíme si, že lze matici $\mathbf{A}$ převést pouze řádkovými úpravami na matici $\mathbf{A}'$, která je tvaru (4.2). Navíc můžeme provádět pouze takové úpravy, které nemění determinant: přičítání násobku jiného řádku k řádku podle (V5) věty 4.21 nemění determinant a pokud potřebujeme prohodit řádky, pak okamžitě pronásobíme jeden z nich konstantou -1. Tyto operace skutečně stačí na převedení matice na tvar (4.2), a přitom máme zaručeno, že $\det \mathbf{A} = \det \mathbf{A}'$. Podle věty 3.55 existuje čtvercová matice $\mathbf{P}$, pro kterou platí

$$\mathbf{A}' = \mathbf{P} \cdot \mathbf{A}.$$

Dále převedeme matici $\mathbf{B}$ na matici $\mathbf{B}'$ tvaru (4.2) pouze sloupcovými úpravami takovými, které nemění determinant. Máme tedy $\det \mathbf{B} = \det \mathbf{B}'$ a navíc podle poznámky 3.58 existuje matice $\mathbf{Q}$ taková, že

$$\mathbf{B}' = \mathbf{B} \cdot \mathbf{Q}.$$

Platí

$$\det \mathbf{A} \det \mathbf{B} = \det \mathbf{A}' \det \mathbf{B}' = \det(\mathbf{A}' \cdot \mathbf{B}').$$

Poslední rovnost ověříme z definice maticového násobení a využijeme toho, že obě matice $\mathbf{A}'$ i $\mathbf{B}'$ jsou tvaru (4.2). Matice $\mathbf{A}' \cdot \mathbf{B}'$ je také tvaru (4.2) a pro její diagonální prvky $g_{i,i}$ platí, že $g_{i,i} = a'_{i,i} b'_{i,i}$. Protože se determinanty matic tvaru (4.2) počítají jako součin prvků na diagonále, máme skutečně $\det \mathbf{A}' \det \mathbf{B}' = \det(\mathbf{A}' \cdot \mathbf{B}')$.

Na matici $\mathbf{A} \cdot \mathbf{B}$ provedeme stejné řádkové a sloupcové úpravy, jako jsme provedli na matice $\mathbf{A}$ resp. $\mathbf{B}$. Dostaneme matici $\mathbf{A}' \cdot \mathbf{B}'$, protože

$$\mathbf{P} \cdot (\mathbf{A} \cdot \mathbf{B}) \cdot \mathbf{Q} = (\mathbf{P} \cdot \mathbf{A}) \cdot (\mathbf{B} \cdot \mathbf{Q}) = \mathbf{A}' \cdot \mathbf{B}'.$$

Provedené řádkové a sloupcové úpravy nemění determinant, takže matice $\mathbf{A}' \cdot \mathbf{B}'$ má stejný determinant jako matice $\mathbf{A} \cdot \mathbf{B}$. Dostáváme výsledek

$$\det \mathbf{A} \det \mathbf{B} = \det \mathbf{A}' \det \mathbf{B}' = \det(\mathbf{A}' \cdot \mathbf{B}') = \det(\mathbf{A} \cdot \mathbf{B}).$$

4.36. Poznámka. Na závěr kapitoly o determinantech předvedeme slíbený důkaz věty 3.50 o existenci inverzní matice pro každou regulární matici. Můžeme to považovat za první praktické využití pojmu determinant. Další využití najdeme v následující kapitole o soustavách lineárních rovnic a dále později při počítání objemů jistých těles.

Existence inverzní matice

Větu 3.50 o existenci inverzní matice zde přepíšeme znovu.

4.37. Věta. Ke čtvercové matici $\mathbf{A}$ existuje inverzní matice právě tehdy, když $\mathbf{A}$ je regulární.

Důkaz. Nechť nejprve $\mathbf{A}$ je singulární, tj. podle věty 4.27 je $\det \mathbf{A} = 0$. Ukážeme, že pak inverzní matice neexistuje. Kdyby existovala (označme ji $\mathbf{A}^{-1}$), pak musí $\mathbf{A} \cdot \mathbf{A}^{-1} = \mathbf{E}$ a podle věty 4.35 je

$$1 = \det \mathbf{E} = \det(\mathbf{A} \cdot \mathbf{A}^{-1}) = \det \mathbf{A} \det \mathbf{A}^{-1} = 0 \cdot \det \mathbf{A}^{-1} = 0,$$

což je spor. Inverzní matice tedy k singulární matici neexistuje.

Nechť nyní $\mathbf{A}$ je regulární. Sestrojíme matici

$$\mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}} \mathbf{B}^T,$$

kde $\mathbf{B} = (D_{i,j})$ je matice doplňků k matici $\mathbf{A}$. Ukážeme, že takto sestrojená $\mathbf{A}^{-1}$ je inverzní matice. Musíme tedy ověřit $\mathbf{A} \cdot \mathbf{A}^{-1} = \mathbf{E}$ a dále $\mathbf{A}^{-1} \cdot \mathbf{A} = \mathbf{E}$. Je-li $\mathbf{B} = (D_{i,j})$, pak samozřejme je $\mathbf{B}^T = (D_{j,i})$. Podle definice součinu matic 3.34 vypočítáme prvek $e_{i,k}$ matice $\mathbf{A} \cdot \mathbf{A}^{-1}$:

$$e_{i,k} = \sum_{j=1}^{n} a_{i,j} \frac{1}{\det \mathbf{A}} D_{k,j} = \frac{1}{\det \mathbf{A}} \big(a_{i,1}D_{k,1} + a_{i,2}D_{k,2} + \cdots + a_{i,n}D_{k,n}\big) = \begin{cases} \dfrac{1}{\det \mathbf{A}} \det \mathbf{A} = 1 & \text{pro } i = k, \\ \dfrac{1}{\det \mathbf{A}} \cdot 0 = 0 & \text{pro } i \neq k. \end{cases}$$

Zde jsme využili větu o rozvoji determinantu podle i-tého řádku, viz poznámku 4.33. Zjišťujeme, že prvky $e_{i,k}$ jsou v souladu s definicí jednotkové matice 3.44. Rovnost $\mathbf{A}^{-1} \cdot \mathbf{A} = \mathbf{E}$ bychom dokazovali podobně. Použili bychom větu o rozvoji i-tého sloupce namísto řádku.

4.38. Věta. Nechť $\mathbf{A}$ je regulární matice. Pak $\det \mathbf{A}^{-1} = 1/\det \mathbf{A}$.

Důkaz. Důkaz jsme vlastně už provedli v první části důkazu předchozí věty. Zopakujeme si to. Protože $\mathbf{E} = \mathbf{A} \cdot \mathbf{A}^{-1}$, musí podle věty 4.35 být $1 = \det \mathbf{E} = \det \mathbf{A} \det \mathbf{A}^{-1}$. Z toho přímo plyne dokazovaný vzorec.

4.39. Poznámka. Důkaz věty 4.37 nám dává návod, jak sestrojit inverzní matici k matici $\mathbf{A}$. Je to vlastně vedle eliminační metody popsané v příkladu 3.53 další metoda hledání inverzní matice. Můžeme ji říkat „metoda hledání inverzní matice pomocí doplňků“. Uvědomíme si ale, že pro velké matice je eliminační metoda podstatně účelnější než metoda pomocí doplňků, která vyžaduje spočítat n^2 determinantů matic typu $(n-1, n-1)$ a ještě spočítat $\det \mathbf{A}$. V následujících příkladech si proto tuto metodu ilustrujeme jen na malých maticích.

4.40. Příklad. Najdeme inverzní matici k matici

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Označme $\mathbf{B}$ matici doplňků k matici $\mathbf{A}$. V tomto případě se doplňky dobře počítají, protože se jedná o determinanty matic typu $(1,1)$:

$$\mathbf{B} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}, \quad \mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}} \mathbf{B}^T = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

4.41. Příklad. Najdeme inverzní matici ke stejné matici, jako v příkladu 3.53, tj. k matici

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ -1 & 0 & 1 \\ 2 & 2 & 1 \end{pmatrix}.$$

Doplňky nyní budeme počítat z determinantů matic typu $(2,2)$, což už nám dá trochu práce.

$$\mathbf{B} = \begin{pmatrix} +\begin{vmatrix} 0 & 1 \\ 2 & 1 \end{vmatrix} & -\begin{vmatrix} -1 & 1 \\ 2 & 1 \end{vmatrix} & +\begin{vmatrix} -1 & 0 \\ 2 & 2 \end{vmatrix} \\ -\begin{vmatrix} 2 & 3 \\ 2 & 1 \end{vmatrix} & +\begin{vmatrix} 1 & 3 \\ 2 & 1 \end{vmatrix} & -\begin{vmatrix} 1 & 2 \\ 2 & 2 \end{vmatrix} \\ +\begin{vmatrix} 2 & 3 \\ 0 & 1 \end{vmatrix} & -\begin{vmatrix} 1 & 3 \\ -1 & 1 \end{vmatrix} & +\begin{vmatrix} 1 & 2 \\ -1 & 0 \end{vmatrix} \end{pmatrix} = \begin{pmatrix} -2 & 3 & -2 \\ 4 & -5 & 2 \\ 2 & -4 & 2 \end{pmatrix},$$

$$\det \mathbf{A} = -2, \qquad \mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}} \mathbf{B}^T = -\frac{1}{2} \begin{pmatrix} -2 & 4 & 2 \\ 3 & -5 & -4 \\ -2 & 2 & 2 \end{pmatrix}.$$

Výsledek můžeme srovnat s výsledkem v příkladu 3.53.

5. Soustavy lineárních rovnic

5.1. Definice. Nechť $\mathbf{A}$ je matice reálných čísel typu (m,n), nechť dále $\boldsymbol{x}$ je jednosloupcová matice symbolů $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ typu $(n,1)$ a $\boldsymbol{b}$ je matice reálných čísel $\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ typu $(m,1)$. Pak maticovou rovnost

$$\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$$

navýváme *soustavou m lineárních rovnic o n neznámých.* Matici $\mathbf{A}$ nazýváme *maticí soustavy* a vektor $\boldsymbol{b}^T = (b_1,\dots,b_m)$ nazýváme *vektorem pravých stran.* Připíšeme-li k matici soustavy do dalšího sloupce matici $\boldsymbol{b}$ oddělenou (pouze pro přehlednost) svislou čarou, dostáváme matici $(\mathbf{A}|\boldsymbol{b})$ typu $(m,n+1)$, kterou nazýváme *rozšířenou maticí soustavy.*

5.2. Definice. *Řešením soustavy* $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ je takový vektor $\boldsymbol{a} = (\alpha_1,\alpha_2,\dots,\alpha_n) \in \mathbf{R}^n$, pro který platí: dosadíme-li hodnoty α_i za symboly x_i, pak je splněna požadovaná maticová rovnost, tj.

$$\mathbf{A}\cdot\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}. \tag{5.1}$$

Řešit soustavu $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ znamená nalézt všechna její řešení, tj. nalézt podmnožinu $\mathbf{R}^n$ všech řešení této soustavy.

5.3. Poznámka. Všimneme si, že z historických důvodů se v rovnosti $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ značí jednosloupcové matice malým písmenem podobně, jako vektory. Často se na tyto matice zjednodušeně díváme jako na prvky z $\mathbf{R}^n$ nebo $\mathbf{R}^m$, jen nesmíme zapomenout, že složky těchto uspořádaných m-tic a n-tic v kontextu rovnosti $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ píšeme do sloupce a nikoli do řádku.

Matice $\boldsymbol{x}$ může místo symbolů $x_1,x_2,\dots,x_n$ obsahovat i jiné symboly, například x,y,z.

5.4. Věta (Frobeniova). Soustava $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ má řešení právě tehdy, když $\operatorname{hod}\mathbf{A} = \operatorname{hod}(\mathbf{A}|\boldsymbol{b})$, tj. když hodnost matice soustavy se rovná hodnosti rozšířené matice soustavy. *Frobeniova věta*

Důkaz. Vektor $\boldsymbol{a} = (\alpha_1,\dots,\alpha_n)$ je řešením soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ právě tehdy, když platí (5.1). To znamená, že sloupec $\boldsymbol{b}$ je lineární kombinací sloupců matice $\mathbf{A}$ s koeficienty $\alpha_1,\alpha_2,\dots,\alpha_n$. To platí právě tehdy, když

$$\operatorname{hod}\begin{pmatrix} \mathbf{A}^T \\ \boldsymbol{b}^T \end{pmatrix} = \operatorname{hod}\mathbf{A}^T.$$

Protože platí věta 3.31, je Frobeniova věta dokázána.

5.5. Poznámka. V úvodní kapitole o Gaussově eliminační metodě jsme vlastně nevědomky vyslovili Frobeniovu větu. V této kapitole jsme si říkali, jak poznáme, že soustava má řešení. Mluvili jsme tam o tom, že soustava nemá řešení právě tehdy, když poslední řádek rozšířené matice soustavy po eliminaci je tvaru

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

Vzpomeneme-li si na metodu počítání hodnosti z příkladu 3.14, vidíme, že existence takového řádku je ekvivalentní s tím, že rozšířená matice soustavy má o jedničku větší hodnost, než matice soustavy. Uvědomíme si ještě, že hodnost rozšířené matice soustavy může být buď o jedničku větší nebo přímo rovna hodnosti matice soustavy. Žádná jiná možnost pro hodnosti těchto matic neexistuje.

5.6. Definice. Nechť $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ je soustava m lineárních rovnic o n neznámých a $\mathbf{C}\,\boldsymbol{x} = \boldsymbol{d}$ je soustava k lineárních rovnic o stejném počtu n neznámých. Říkáme, že tyto soustavy jsou *ekvivalentní*, pokud obě soustavy mají stejné množiny řešení.

Princip eliminační metody

5.7. Poznámka. Gaussova eliminační metoda řešení soustav lineárních rovnic popsaná v úvodní kapitole spočívá vlastně v převedení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ na soustavu $\mathbf{C}\,\boldsymbol{x} = \boldsymbol{d}$, která je s původní soustavou rovnic ekvivalentní. Přitom řešení soustavy $\mathbf{C}\,\boldsymbol{x} = \boldsymbol{d}$ lze nalézt snadněji, protože $\mathbf{C}$ je horní trojúhelníková matice (srovnejte větu 3.23). Tuto skutečnost zaznamenáme do následující věty.

5.8. Věta. Ke každé soustavě $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ lze nalézt ekvivalentní soustavu $\mathbf{C}\,\boldsymbol{x} = \boldsymbol{d}$, jejíž matice $\mathbf{C}$ je horní trojúhelníková.

Důkaz. Podle věty 3.23 lze nalézt $(\mathbf{C}|\boldsymbol{d})$ takovou, že $(\mathbf{A}|\boldsymbol{b}) \sim (\mathbf{C}|\boldsymbol{d})$, a přitom $\mathbf{C}$ je horní trojúhelníková matice. Protože operace „$\sim$“ zde označuje konečně mnoho elementárních kroků Gaussovy eliminační metody, a protože jsme si řekli v úvodní kapitole, že tyto elementární kroky nemění množinu řešení odpovídající soustavy, je soustava $\mathbf{C}\,\boldsymbol{x} = \boldsymbol{d}$ ekvivalentní s původní soustavou $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$.

Řešení homogenní soustavy

5.9. Definice. Existuje-li v matici $\boldsymbol{b}$ aspoň jeden prvek nenulový, říkáme, že je soustava lineárních rovnic $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ *nehomogenní.* Jsou-li všechny prvky v matici $\boldsymbol{b}$ nulové, nazýváme soustavu rovnic *homogenní* a zapisujeme ji takto:

$$\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o} \qquad \text{(symbolem } \boldsymbol{o} \text{ nyní značíme jednosloupcovou nulovou matici).}$$

5.10. Věta. Množina všech řešení homogenní soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$ s n neznámými tvoří lineární podprostor lineárního prostoru $\mathbf{R}^n$.

Důkaz. Především množina řešení homogenní soustavy je neprázdná, protože nulový vektor v $\mathbf{R}^n$ je samozřejmě řešením této soustavy.

Podle definice 1.17 musíme dále dokázat: (1) jsou-li $\boldsymbol{u} \in \mathbf{R}^n$ a $\boldsymbol{v} \in \mathbf{R}^n$ řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$, pak též $\boldsymbol{u} + \boldsymbol{v}$ je řešením stejné soustavy. (2) je-li $\boldsymbol{u} \in \mathbf{R}^n$ řešením soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$ a $\alpha \in \mathbf{R}$, pak též $\alpha\,\boldsymbol{u}$ je řešením stejné soustavy. Pro účely důkazu označme symbolem $\boldsymbol{u}^T$ jednosloupcovou matici, jejíž prvky odpovídají složkám vektoru $\boldsymbol{u}$. Podobně $\boldsymbol{v}^T$ je sloupec vzniklý z vektoru $\boldsymbol{v}$.

Protože $\boldsymbol{u}$ a $\boldsymbol{v}$ jsou řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$, platí: $\mathbf{A}\,\boldsymbol{u}^T = \boldsymbol{o}$ a $\mathbf{A}\,\boldsymbol{v}^T = \boldsymbol{o}$. Máme dokázat, že $\mathbf{A}\,(\boldsymbol{u}^T + \boldsymbol{v}^T) = \boldsymbol{o}$ a $\mathbf{A}\,(\alpha\,\boldsymbol{u}^T) = \boldsymbol{o}$. Podle věty 3.38 je

$$\begin{gathered}\mathbf{A}\,(\boldsymbol{u}^T + \boldsymbol{v}^T) = \mathbf{A}\,\boldsymbol{u}^T + \mathbf{A}\,\boldsymbol{v}^T = \boldsymbol{o} + \boldsymbol{o} = \boldsymbol{o},\\ \mathbf{A}\,(\alpha\,\boldsymbol{u}^T) = \alpha\,\mathbf{A}\,\boldsymbol{u}^T = \alpha\,\boldsymbol{o} = \boldsymbol{o}.\end{gathered}$$

5.11. Příklad. Najdeme množinu všech řešení homogenní soustavy lineárních rovnic se šesti neznámými:

$$\begin{aligned} x_1 + x_2 + 2x_3 + 3x_4 + 3x_5 + 3x_6 &= 0\\ x_1 + x_2 + x_3 + 3x_4 + x_5 + x_6 &= 0\\ 2x_1 + 2x_2 + 2x_3 + 6x_4 + 2x_5 + 8x_6 &= 0 \end{aligned}$$

Eliminujeme matici soustavy (vektor pravých stran je nulový, takže je zbytečné jej psát).

$$\begin{pmatrix} 1&1&2&3&3&3\\ 1&1&1&3&1&1\\ 2&2&2&6&2&8 \end{pmatrix} \sim \begin{pmatrix} 1&1&2&3&3&3\\ 0&0&-1&0&-2&-2\\ 0&0&-2&0&-4&2 \end{pmatrix} \sim \begin{pmatrix} 1&1&2&3&3&3\\ 0&0&1&0&2&2\\ 0&0&0&0&0&6 \end{pmatrix}.$$

Z poslední rovnice budeme počítat x_6, z předposlední rovnice x_3 a z první rovnice x_1. Hodnoty neznámých x_2, x_4, x_5 mohou být libovolné. Zaveďme pro ně parametry $x_2 = t$, $x_4 = u$, $x_5 = v$. Z poslední rovnice vychází jedině $x_6 = 0$, z předposlední rovnice máme $x_3 = -2v$ a konečně z první rovnice dostáváme $x_1 = -t + 4v - 3u - 3v = -t + v - 3u$. Výsledek sumarizujeme takto:

$$\begin{aligned}(x_1, x_2, x_3, x_4, x_5, x_6) &= (-t + v - 3u,\ t,\ -2v,\ u,\ v,\ 0) =\\ &= t\,(-1, 1, 0, 0, 0, 0) + u\,(-3, 0, 0, 1, 0, 0) + v\,(1, 0, -2, 0, 1, 0).\end{aligned}$$

Z tohoto zápisu vyplývá, že množina všech řešení dané homogenní soustavy je množinou všech lineárních kombinací uvedených tří vektorů, což můžeme zapsat pomocí lineárního obalu takto:

$$M_0 = \big\langle (-1, 1, 0, 0, 0, 0), (-3, 0, 0, 1, 0, 0), (1, 0, -2, 0, 1, 0) \big\rangle.$$

5.12. Poznámka. Protože uvedené tři vektory z výsledku příkladu 5.11 jsou lineárně nezávislé, tvoří jednu z možných bází prostoru M_0. To se nestalo náhodou, ale platí to vždy, jak ukazuje následující věta.

5.13. Věta. Nechť $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$ je homogenní soustava lineárních rovnic o n neznámých, $k = n - \operatorname{hod}\mathbf{A}$. Pak existuje k lineárně nezávislých vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ z $\mathbf{R}^n$ takových, že pro množinu M_0 všech řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$ platí

$$M_0 = \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle.$$

Vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ tvoří jednu z možných bází lineárního prostoru všech řešení M_0.

Důkaz. Vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ najdeme analogicky, jako jsme to udělali v příkladu 5.11. Podle poznámky 3.24 je počet rovnic soustavy po eliminaci roven $\operatorname{hod}\mathbf{A}$ a je roven počtu neznámých, které můžeme z rovnic vypočítat. Ostatních $k = n - \operatorname{hod}\mathbf{A}$ neznámých $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$ může nabývat libovolných hodnot a zaveďme pro ně parametry $x_{i_1} = p_1, x_{i_2} = p_2, \ldots, x_{i_k} = p_k$. Všechna řešení získáme například dosazovací metodou použitou na rovnice po eliminaci (začínáme poslední rovnicí a končíme první). Z tohoto řešení můžeme vytknout parametry:

$$(x_1, x_2, \ldots, x_n) = p_1\,\boldsymbol{u}_1 + p_2\,\boldsymbol{u}_2 + \cdots + p_k\,\boldsymbol{u}_k \tag{5.2}$$

a dostáváme hledané vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$. Z uvedené rovnosti a z definice lineárního obalu 2.29 přímo plyne, že pro množinu všech řešení platí $M_0 = \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle$.

Zbývá dokázat, že vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ jsou lineárně nezávislé. Označme $\boldsymbol{u}'_1 \in \mathbf{R}^k$, $\boldsymbol{u}'_2 \in \mathbf{R}^k, \ldots,$ $\boldsymbol{u}'_k \in \mathbf{R}^k$ ty části vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$, které obsahují jen složky $i_1, i_2, \ldots, i_k$. Protože platí rovnost (5.2) a také platí označení $x_{i_1} = p_1, x_{i_2} = p_2, \ldots, x_{i_k} = p_k$, dostáváme

$$\boldsymbol{u}'_1 = (1,0,0,\ldots,0), \quad \boldsymbol{u}'_2 = (0,1,0,\ldots,0), \quad \ldots, \quad \boldsymbol{u}'_k = (0,0,0,\ldots,1).$$

Toto jsou lineárně nezávislé vektory. Z toho plyne, že jsou lineárně nezávislé i vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$, 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 řešení homogenní soustavy, plyne přímo z definice báze 2.42.

5.14. Věta. Nechť M_0 je lineární prostor všech řešení homogenní soustavy lineárních rovnic $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$ s n neznámými. Pak $\dim M_0 = n - \operatorname{hod}\mathbf{A}$.

Důkaz. Věta je přímým důsledkem předchozí věty.

5.15. Poznámka. Nechť n je počet neznámých homogenní soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$. Pak z věty 5.14 plyne tento důsledek:

$\operatorname{hod}\mathbf{A} = n$ pak soustava má jen nulové řešení,

$\operatorname{hod}\mathbf{A} < n$ pak soustava má nekonečně mnoho řešení.

5.16. Poznámka. Když jsme procvičovali definici lineární závislosti a nezávislosti (viz příklady za definicí 2.7 a 2.9), zadání vždy vedlo na homogenní soustavu lineárních rovnic, která má vždy aspoň nulové řešení. V příkladech šlo o to, zda soustava má i jiné než nulové řešení, tj. zda hodnost matice soustavy je menší než počet neznámých.

5.17. Definice. Nechť $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ je nehomogenní soustava lineárních rovnic o n neznámých a $\boldsymbol{v} \in \mathbf{R}^n$ je nějaké jedno její řešení. Takovému řešení $\boldsymbol{v}$ říkáme *partikulární řešení* nehomogenní soustavy.

Řešení nehomogenní soustavy

Pokud zaměníme matici $\boldsymbol{b}$ za nulovou matici stejného typu, dostáváme homogenní soustavu $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$, kterou nazýváme *přidruženou homogenní soustavou* k soustavě $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$.

5.18. Věta. (1) Nechť $\boldsymbol{v}$ je partikulární řešení nehomogenní soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ a $\boldsymbol{u}$ je libovolné řešení přidružené homogenní soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$. Pak $\boldsymbol{v} + \boldsymbol{u}$ je také řešením soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$.

(2) Nechť $\boldsymbol{v}$ a $\boldsymbol{w}$ jsou dvě partikulární řešení nehomogenní soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$. Pak $\boldsymbol{v} - \boldsymbol{w}$ je řešením přidružené homogenní soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$.

Důkaz. Označme (stejně jako v důkazu věty 5.10) symbolem $\boldsymbol{v}^T$ jednosloupcovou matici, která obsahuje složky vektoru $\boldsymbol{v}$. Analogicky označme $\boldsymbol{u}^T$ a $\boldsymbol{w}^T$.
(1) Podle předpokladu platí $\mathbf{A}\,\boldsymbol{v}^T = \boldsymbol{b}$, $\mathbf{A}\,\boldsymbol{u}^T = \boldsymbol{o}$. Pro součet $\boldsymbol{v} + \boldsymbol{u}$ pak platí

$$\mathbf{A}\,(\boldsymbol{v}^T + \boldsymbol{u}^T) = \mathbf{A}\,\boldsymbol{v}^T + \mathbf{A}\,\boldsymbol{u}^T = \boldsymbol{b} + \boldsymbol{o} = \boldsymbol{b}.$$

(2) Podle předpokladu platí $\mathbf{A}\,\boldsymbol{v}^T = \boldsymbol{b}$, $\mathbf{A}\,\boldsymbol{w}^T = \boldsymbol{b}$. Pro rozdíl $\boldsymbol{v} - \boldsymbol{w}$ pak platí

$$\mathbf{A}\,(\boldsymbol{v}^T - \boldsymbol{w}^T) = \mathbf{A}\,\boldsymbol{v}^T - \mathbf{A}\,\boldsymbol{w}^T = \boldsymbol{b} - \boldsymbol{b} = \boldsymbol{o}.$$

5.19. Věta. Nechť $\boldsymbol{v}$ je partikulární řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ a M_0 je lineární prostor všech řešení přidružené homogenní soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$. Pak pro množinu M všech řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ platí

$$M = \big\{\boldsymbol{v} + \boldsymbol{u};\ \ \boldsymbol{u} \in M_0\big\}.$$

Důkaz. Z vlastnosti (1) věty 5.18 plyne, že $\{\boldsymbol{v} + \boldsymbol{u};\ \ \boldsymbol{u} \in M_0\} \subseteq M$. Stačí dokázat obrácenou inkluzi. Pokud $\boldsymbol{w} \in M$, pak podle vlastnosti (2) věty 5.18 existuje $\boldsymbol{u} = \boldsymbol{w} - \boldsymbol{v} \in M_0$, takže $\boldsymbol{w} \in \{\boldsymbol{v}+\boldsymbol{u};\ \ \boldsymbol{u} \in M_0\}$. Platí tedy i obrácenná inkluze.

5.20. Poznámka. Množinu všech řešení nehomogenní soustavy lineárních rovnic zapisujeme většinou zjednodušeně jako součet partikulárního řešení a lineárního prostoru všech řešení přidružené homogenní soustavy takto:

$$M = \boldsymbol{v} + M_0 = \boldsymbol{v} + \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k\rangle. \tag{5.3}$$

Řešit nehomogenní soustavu tedy znamená najít partikulární řešení $\boldsymbol{v}$ a dále najít k lineárně nezávislých řešení přidružené homogenní soustavy $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ (k je rovno počtu neznámých mínus hodnost matice soustavy). Výsledek je obvyklé psát ve tvaru (5.3).

5.21. Poznámka. Při strojovém zpracování rozsáhlých soustav většinou jde o to najít jedno partikulární řešení a bázi prostoru řešení přidružené homogenní soustavy. Přitom není nutné programovat symbolické výpočty, jako je například vytýkání parametrů podle rovnosti (5.2). Můžeme na to jít jinak. *Strojové řešení soustav*

Nejprve eliminujeme rozšířenou matici soustavy na horní trojúhelníkovou a rozhodneme, které sloupce matice odpovídají proměnným, které budeme z rovnic počítat (většinou podle prvního nenulového prvku v každém řádku). Ostatní sloupce označíme $i_1, i_2, \ldots, i_k$ jako v důkazu věty 5.13.

Nechť $\boldsymbol{c} \in \mathbf{R}^k$ je vektor hodnot řešení ve složkách $i_1, i_2, \ldots, i_k$. Volíme nejprve $\boldsymbol{c} = (0, 0, \ldots, 0)$ a dopočítáme z rovnic ostatní složky řešení. Dostáváme partikulární řešení $\boldsymbol{v}$. Dále zaměníme vektor pravých stran za nulový vektor (přecházíme k přidružené homogenní soustavě). Volíme postupně

$$\boldsymbol{c} = (1, 0, \ldots, 0), \quad \boldsymbol{c} = (0, 1, \ldots, 0), \quad \ldots, \quad \boldsymbol{c} = (0, 0, \ldots, 1) \tag{5.4}$$

a pro každé takové zadání vektoru $\boldsymbol{c}$ dopočítáme ostatní složky vektoru řešení. Dostáváme tak postupně vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$. Množinu všech řešení pak můžeme zapsat stejně, jako ve vzorci (5.3).

5.22. Poznámka. Na malých modelových příkladech (soustavy s malým počtem rovnic a neznámých) většinou nemusíme použít strojové zpracovámí a můžeme řešení počítat „ručně“. Pak se jeví výhodnější zavést parametry a vytknout je (podobně jako v příkladu 5.11) a nedělat při výpočtu zbytečné přechody na přidruženou homogenní soustavu. Oba dva přístupy (strojový i lidský) si ukážeme na následujícím příkladě.

5.23. Příklad. Najdeme množinu všech řešení soustavy lineárních rovnic se šesti neznámými:

$$\begin{aligned}
x_1 + \ \ x_2 + 2x_3 + 3x_4 + 3x_5 + 3x_6 &= \ \ \ 1\\
x_1 + \ \ x_2 + \ \ x_3 + 3x_4 + \ \ x_5 + \ \ x_6 &= -1\\
2x_1 + 2x_2 + 2x_3 + 6x_4 + 2x_5 + 8x_6 &= \ 10
\end{aligned}$$

Eliminujeme rozšířenou matici soustavy.

$$\left(\begin{array}{cccccc|c} 1&1&2&3&3&3&1\\ 1&1&1&3&1&1&-1\\ 2&2&2&6&2&8&10 \end{array}\right) \sim \left(\begin{array}{cccccc|c} 1&1&2&3&3&3&1\\ 0&0&-1&0&-2&-2&-2\\ 0&0&-2&0&-4&2&8 \end{array}\right) \sim \left(\begin{array}{cccccc|c} 1&1&2&3&3&3&1\\ 0&0&1&0&2&2&2\\ 0&0&0&0&0&6&12 \end{array}\right) \sim \left(\begin{array}{cccccc|c} 1&1&2&3&3&3&1\\ 0&0&1&0&2&2&2\\ 0&0&0&0&0&1&2 \end{array}\right).$$

Nejprve ukážeme doporučený postup pro „ruční počítání“.

Z poslední rovnice budeme počítat x_6, z předposlední rovnice x_3 a z první rovnice x_1. Hodnoty neznámých x_2, x_4, x_5 mohou být libovolné. Zaveďme pro ně parametry $x_2 = t$, $x_4 = u$, $x_5 = v$.

Z poslední rovnice máme $x_6 = 2$, z předposlední rovnice $x_3 = 2 - 2v - 2 \cdot 2 = -2 - 2v$ a konečně z první rovnice dostáváme $x_1 = 1 - t - 2(-2 - 2v) - 3u - 3v - 3 \cdot 2 = -1 - t + v - 3u$. Výsledek sumarizujeme takto:

$$\begin{aligned}
(x_1, x_2, x_3, x_4, x_5, x_6) &= (-1 - t + v - 3u, t, -2 - 2v, u, v, 2) =\\
&= (-1, 0, -2, 0, 0, 2) + t\,(-1, 1, 0, 0, 0, 0) + u\,(-3, 0, 0, 1, 0, 0) + v\,(1, 0, -2, 0, 1, 0).
\end{aligned}$$

Z tohoto zápisu vyplývá, že množina všech řešení dané nehomogenní soustavy je rovna

$$M = (-1, 0, -2, 0, 0, 2) + \big\langle(-1, 1, 0, 0, 0, 0), (-3, 0, 0, 1, 0, 0), (1, 0, -2, 0, 1, 0)\big\rangle.$$

Vektor $(-1, 0, -2, 0, 0, 2)$ je partikulárním řešením dané nehomogenní soustavy a vektory $(-1, 1, 0, 0, 0, 0)$, $(-3, 0, 0, 1, 0, 0)$, $(1, 0, -2, 0, 1, 0)$ tvoří bázi prostoru řešení přidružené homogenní soustavy.

5.24. Příklad. Je dána stejná soustava lineárních rovnic jako v příkladu 5.23. Ukážeme postup řešení vhodný pro strojové zpracování. Po eliminaci dostáváme matici

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

Šipkami jsou označeny sloupce, které odpovídají neznámým s libovomými hodnotami. Do nich budeme dosazovat postupně hodnoty $(0,0,0)$ při daném vektoru pravých stran a dále $(1,0,0)$, $(0,1,0)$ a $(0,0,1)$ při nulovém vektoru pravých stran. V prvním případě dopočítáme složky partikulárního řešení $\boldsymbol{v}$. Víme, že je $\boldsymbol{v} = (?,0,?,0,0,?)$. Zbylé složky označené otazníkem spočítáme z následující soustavy (dosazením nul sloupce vyznačené šipkami vymizí):

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 2 \end{array}\right) \sim \left(\begin{array}{ccc|r} 1 & 2 & 0 & -5 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 2 \end{array}\right) \sim \left(\begin{array}{ccc|r} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 2 \end{array}\right), \quad \text{je tedy } \boldsymbol{v} = (-1,0,-2,0,0,2).$$

Nyní budeme počítat neznámé složky pro $\boldsymbol{u}_1 = (?,1,?,0,0,?)$. Na pravé straně jsou nyní nuly, protože počítáme řešení přidružené homogenní soustavy. Po dosazení jedničky ve druhém sloupci a převedení konstant na pravou stranu rovnic dostáváme nakonec na pravé straně „mínus druhý sloupec", tj.

$$\left(\begin{array}{ccc|r} 1 & 2 & 3 & -1 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|r} 1 & 2 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|r} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right), \quad \text{je tedy } \boldsymbol{u}_1 = (-1,1,0,0,0,0).$$

Všimneme si, že jsme vlastně řešili stejnou soustavu tří rovnic o třech neznámých, jako v případě vektoru $\boldsymbol{v}$, jen pravá strana se lišila. Podobné by to bylo i pro ostatní vektory $\boldsymbol{u}_2, \boldsymbol{u}_3$. Je výhodné napsat všechny vektory pravých stran vedle sebe za svislou čáru a řešit tak všechny soustavy najednou. Pro úplnost vyřešíme znovu i $\boldsymbol{v}$ a $\boldsymbol{u}_1$.

$$\boldsymbol{v} = (?,0,?,0,0,?), \quad \boldsymbol{u}_1 = (?,1,?,0,0,?), \quad \boldsymbol{u}_2 = (?,0,?,1,0,?), \quad \boldsymbol{u}_3 = (?,0,?,0,1,?),$$

$$\left(\begin{array}{ccc|rrrr} 1 & 2 & 3 & 1 & -1 & -3 & -3 \\ 0 & 1 & 2 & 2 & 0 & 0 & -2 \\ 0 & 0 & 1 & 2 & 0 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|rrrr} 1 & 2 & 0 & -5 & -1 & -3 & -3 \\ 0 & 1 & 0 & -2 & 0 & 0 & -2 \\ 0 & 0 & 1 & 2 & 0 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|rrrr} 1 & 0 & 0 & -1 & -1 & -3 & 1 \\ 0 & 1 & 0 & -2 & 0 & 0 & -2 \\ 0 & 0 & 1 & 2 & 0 & 0 & 0 \end{array}\right),$$

$$\boldsymbol{v} = (-1,0,-2,0,0,2), \quad \boldsymbol{u}_1 = (-1,1,0,0,0,0), \quad \boldsymbol{u}_2 = (-3,0,0,1,0,0), \quad \boldsymbol{u}_3 = (1,0,-2,0,1,0),$$

$$M = (-1,0,-2,0,0,2) + \big\langle (-1,1,0,0,0,0), (-3,0,0,1,0,0), (1,0,-2,0,1,0) \big\rangle.$$

Nejednoznačnost zápisu řešení

5.25. Poznámka. Již v úvodní kapitole o Gaussově eliminační metodě jsme zmínili, že množinu řešení soustavy lineárních rovnic neumíme popsat jednoznačným způsobem. Výjimkou je pouze případ, kdy má soustava jediné řešení. Víme totiž, že každý netriviální lineární podprostor má nekonečně mnoho bází a má-li soustava více řešení, pak i partikulární řešení může každý zapsat jiné.

K různým zápisům téže množiny řešení můžeme dospět při výpočtu třeba tak, že volíme rozdílnou skupinu neznámých, které mohou nabývat libovolných hodnot. I při stejné skupině těchto neznámých nás nikdo nenutí, abychom volili výchozí hodnoty pro tyto neznámé jen jedničky a nuly způsobem, jak bylo uvedeno v (5.4). V modelových řešeních modelových příkladů ze skript se můžeme setkat někdy i s jinými výchozími hodnotami volenými tak, aby výsledek vyšel bez použití zlomků pouze s malými celými čísly. Tuto dovednost nebudeme v praktických příkladech (které nejsou modelové) potřebovat, takže nás nemusí frustrovat, že nám vycházejí ve výsledcích zlomky. Metodu, jak získat výsledek za každou cenu zapsaný pomocí malých celých čísel, ve svém textu nezmiňuji, protože ji nepovažuji za důležitou.

Může nás ale zajímat, zda náš výsledek a výsledek, který třeba najdeme ve skriptech, popisují stejnou množinu řešení. Jak to poznáme? Především báze prostoru řešení přidružené homogenní soustavy musí obsahovat v obou výsledcích podle věty 2.59 stejný počet prvků. Ověříme ještě, že jsou v obou výsledcích skutečně báze, tj. že jsou vektory popisující prostor řešení přidružené homogenní soustavy skutečně lineárně nezávislé. Dále zjistíme, zda oba výsledky popisují stejný podprostor řešení přidružené homogenní soustavy. Jedna z možností, jak to zjistit, je dosadit do soustavy (jednodušeji se dosazuje do soustavy po eliminaci) všechny vektory prověřované báze prostoru řešení přidružené homogenní soustavy. Měl by pro všechny případy vyjít nulový vektor pravých stran. Pak dosadíme ještě partikulární řešení a měl by vyjít vektor pravých stran dané soustavy.

5.26. Poznámka. Co uděláme, pokud se nám dostanou do ruky dva zápisy řešení nějaké soustavy lineárních rovnic, a přitom nemáme k dispozici původní soustavu a nemůžeme tedy dosazovat? Jak v tomto případě poznáme, že oba zápisy popisují stejné řešení? Jsou dány třeba tyto zápisy:

$$\boldsymbol{v} + \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle \stackrel{?}{=} \boldsymbol{w} + \langle \boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_k \rangle$$

Nejprve ověříme lineární nezávislost vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ a lineární nezávislost vektorů $\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_k$. Dále zjistíme, zda jsou rovny lineární obaly. Ověříme, zda $\boldsymbol{g}_i \in \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle$, $\forall i \in \{1, \ldots, k\}$. Jinými slovy je třeba zjistit, zda $\boldsymbol{g}_i$ se dá zapsat jako lineární kombinace vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$. Tím máme zaručenu rovnost lineárních obalů. Díky vlastnosti (3) věty 2.64 není třeba ověřovat $\boldsymbol{u}_i \in \langle \boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_k \rangle$. Nakonec zjistíme, zda obě partikulární řešení popisují stejnou množinu řešení třeba podle vlastnosti (2) věty 5.18 tímto testem: $\boldsymbol{v} - \boldsymbol{w} \in \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle$.

Ověřování $\boldsymbol{g}_i \in \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle$, $\forall i \in \{1, \ldots, k\}$ vede na k soustav lineárních rovnic, což je poměrně pracné (pokud ovšem nejsou koeficienty lineární kombinace snadno vidět díky přítomnosti nul ve složkách vektorů). Je proto někdy výhodnější použít větu 3.13. Podle této věty hodnost matice $\mathbf{C}$ zapsané zde vpravo musí být rovna k. To je postačující pro rovnost množin řešení. Protože pro velká k je matice $\mathbf{C}$ „příliš vysoká“, je někdy výhodné místo toho počítat hodnost matice $\mathbf{C}^T$. Podle věty 3.31 dostaneme stejný výsledek, ale navíc šetříme papírem a dalšími kancelářskými technologiemi.

$$\mathbf{C} = \begin{pmatrix} \boldsymbol{u}_1 \\ \boldsymbol{u}_2 \\ \vdots \\ \boldsymbol{u}_k \\ \boldsymbol{g}_1 \\ \boldsymbol{g}_2 \\ \vdots \\ \boldsymbol{g}_k \\ \boldsymbol{v} - \boldsymbol{w} \end{pmatrix}$$

5.27. Příklad. Prověříme, zda množina

$$M_1 = (1,2,-4,-1,1,2) + \big\langle (7,1,-4,-2,2,0), (-8,3,-2,2,1,0), (2,-2,-6,1,3,0) \big\rangle$$

je rovna množině M z příkladu 5.24.

Díky tomu, že naše řešení z příkladu 5.24 obsahuje na pozicích 2, 4 a 5 systematicky rozmístěné nuly a jedničky, můžeme okamžitě pohledem do těchto pozic psát následující koeficienty lineárních kombinací:

$$\begin{aligned}
(7,1,-4,-2,2,0) &= 1\,(-1,1,0,0,0,0) - 2\,(-3,0,0,1,0,0) + 2\,(1,0,-2,0,1,0),\\
(-8,3,-2,2,1,0) &= 3\,(-1,1,0,0,0,0) + 2\,(-3,0,0,1,0,0) + 1\,(1,0,-2,0,1,0),\\
(2,-2,-6,1,3,0) &= -2\,(-1,1,0,0,0,0) + 1\,(-3,0,0,1,0,0) + 3\,(1,0,-2,0,1,0),\\
(1,2,-4,-1,1,2) &= (-1,0,-2,0,0,2) + 2\,(-1,1,0,0,0,0) - 1\,(-3,0,0,1,0,0) + 1\,(1,0,-2,0,1,0).
\end{aligned}$$

Tyto rovnosti platí i v ostatních složkách (nejen ve složkách 2, 4 a 5) a můžeme tedy prohlásit, že $M_1 = M$.

Pro porovnání zkusíme ještě metodu počítání hodnosti matice $\mathbf{C}$ z poznámky 5.26. Nejprve musíme ověřit, zda jsou vektory $(7,1,-4,-2,2,0), (-8,3,-2,2,1,0), (2,-2,-6,1,3,0)$ lineárně nezávislé (například eliminací třířádkové matice obsahující tyto vektory). Zjistíme, že jsou lineárně nezávislé. Pak spočítáme hodnost matice $\mathbf{C}$:

$$\mathbf{C}^T = \begin{pmatrix} -1 & -3 & 1 & 7 & -8 & 2 & -2 \\ 1 & 0 & 0 & 1 & 3 & -2 & -2 \\ 0 & 0 & -2 & -4 & -2 & -6 & 2 \\ 0 & 1 & 0 & -2 & 2 & 1 & 1 \\ 0 & 0 & 1 & 2 & 1 & 3 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} -1 & -3 & 1 & 7 & -8 & 2 & -2 \\ 0 & -3 & 1 & 8 & -5 & 0 & -4 \\ 0 & 1 & 0 & -2 & 2 & 1 & 1 \\ 0 & 0 & -2 & -4 & -2 & -6 & 2 \\ 0 & 0 & 1 & 2 & 1 & 3 & -1 \end{pmatrix} \sim \begin{pmatrix} -1 & -3 & 1 & 7 & -8 & 2 & -2 \\ 0 & -3 & 1 & 8 & -5 & 0 & -4 \\ 0 & 0 & 1 & 2 & 1 & 3 & -1 \end{pmatrix}.$$

Je $\operatorname{hod} \mathbf{C} = 3$, takže platí $M = M_1$.

5.28. Poznámka. Je-li $\mathbf{A}$ čtvercová matice, pak je výhodné při řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ spočítat $\det \mathbf{A}$.

Soustavy se čtvercovou maticí

Pro $\det \mathbf{A} \neq 0$ je $\operatorname{hod} \mathbf{A}$ rovna počtu neznámých, tj. matice $\mathbf{A}$ je regulární a soustava má jediné řešení. Podle věty 4.37 existuje inverzní matice, takže po vynásobení rovnosti $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ inverzní maticí $\mathbf{A}^{-1}$ zleva máme okamžitě řešení této soustavy $\boldsymbol{x} = \mathbf{A}^{-1}\,\boldsymbol{b}$. Navíc můžeme použít pro zjištění jednotlivých složek řešení tzv. Cramerovo pravidlo (viz následující větu).

Pro $\det \mathbf{A} = 0$ je $\operatorname{hod} \mathbf{A}$ menší než počet neznámých. Pokud má tato soustava podle Frobeniovy věty 5.4 řešení, pak po eliminaci a odstranění nulových řádků dostáváme soustavu, která už nemá čtvercovou matici. V tomto případě nezbývá nic jiného, než použít postup pro nalezení všech řešení, který byl již vyložen dříve.

5.29. Věta (Cramerovo pravidlo). Nechť $\mathbf{A}$ je regulární čtvercová matice. Pak pro i-tou složku řešení soustavy $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{b}$ platí

$$\alpha_i = \frac{\det \mathbf{B}_i}{\det \mathbf{A}}\,,$$

kde matice $\mathbf{B}_i$ je shodná s maticí $\mathbf{A}$ až na i-tý sloupec, který je zaměněn za sloupec pravých stran.

Důkaz. Víme, že platí $\boldsymbol{x} = \mathbf{A}^{-1}\,\boldsymbol{b}$. Podle důkazu věty 4.37 o existenci inverzní matice platí

$$\mathbf{A}^{-1} = (c_{i,j}) = \left(\frac{D_{j,i}}{\det \mathbf{A}}\right), \quad \text{kde } D_{i,j} \text{ je matice doplňků k matici } \mathbf{A}.$$

Nechť b_i jsou složky sloupce $\boldsymbol{b}$. Podle definice maticového násobení je

$$\alpha_i = \sum_{j=1}^{n} c_{i,j}\,b_j = \sum_{j=1}^{n} \frac{D_{j,i}}{\det \mathbf{A}}\,b_j = \frac{1}{\det \mathbf{A}}\Big(D_{1,i}\,b_1 + D_{2,i}\,b_2 + \cdots + D_{k,i}\,b_k\Big) = \frac{\det \mathbf{B}_i}{\det \mathbf{A}}.$$

V poslední rovnosti jsme využili větu o rozvoji determinantu matice $\mathbf{B}_i$ podle i-tého sloupce, viz poznámku 4.33.

5.30. Příklad. Při řešení soustavy

$$\begin{pmatrix} 1 & 2 & 3\\ 3 & 4 & 5\\ 5 & 6 & 8 \end{pmatrix} \cdot \begin{pmatrix} x_1\\ x_2\\ x_3 \end{pmatrix} = \begin{pmatrix} 10\\ 11\\ 12 \end{pmatrix}$$

použijeme Cramerovo pravidlo. Dostáváme:

$$x_1 = \frac{1}{D}\begin{vmatrix} 10 & 2 & 3\\ 11 & 4 & 5\\ 12 & 6 & 8 \end{vmatrix}, \quad x_2 = \frac{1}{D}\begin{vmatrix} 1 & 10 & 3\\ 3 & 11 & 5\\ 5 & 12 & 8 \end{vmatrix}, \quad x_3 = \frac{1}{D}\begin{vmatrix} 1 & 2 & 10\\ 3 & 4 & 11\\ 5 & 6 & 12 \end{vmatrix}, \quad \text{kde } D = \begin{vmatrix} 1 & 2 & 3\\ 3 & 4 & 5\\ 5 & 6 & 8 \end{vmatrix}.$$

Vypočítáním čtyř determinantů z uvedených matic typu (3,3) dostáváme výsledek

$$x_1 = \frac{18}{-2} = -9, \quad x_2 = \frac{-19}{-2} = \frac{19}{2}, \quad x_3 = \frac{0}{-2} = 0, \quad (x_1, x_2, x_3) = \left(-9, \frac{19}{2}, 0\right).$$

5.31. Poznámka. Cramerovo pravidlo se nejeví pro výpočet řešení soustavy s regulární maticí příliš účelné. Potřebujeme spočítat $n+1$ determinantů matic typu (n,n), což je pro velká n náročnější, než spočítat inverzní matici eliminační metodou. Výhodná může být tato metoda pouze tehdy, když nepotřebujeme znát všechny složky řešení, ale jen některé. Například můžeme mít nějaký fyzikální model vyjádřený rozsáhlou soustavou lineárních rovnic, přičemž z mnoha stovek výstupních veličin (tj. složek řešení) nás zajímá jen pár.

5.32. Příklad. Budeme řešit soustavu lineárních rovnic

$$\begin{aligned} x + py + z &= 1\\ x + 2y + z &= -1\\ y + pz &= -1 \end{aligned}$$

Rozlišíme různé množiny řešení této soustavy podle hodnot reálného parametru p.

Determinant matice soustavy je roven $D = p\,(2-p)$, takže pro $p \neq 0$ a $p \neq 2$ je matice soustavy regulární a soustava má jediné řešení. Například Cramerovým pravidlem zjistíme toto řešení:

$$x = \frac{1}{D}\begin{vmatrix} 1 & p & 1\\ -1 & 2 & 1\\ -1 & 1 & p \end{vmatrix} = \frac{p+1}{2-p}, \quad y = \frac{1}{D}\begin{vmatrix} 1 & 1 & 1\\ 1 & -2 & 0\\ 0 & -1 & p \end{vmatrix} = \frac{2}{p-2}, \quad z = \frac{1}{D}\begin{vmatrix} 1 & p & 1\\ 1 & 2 & -1\\ 0 & 1 & -1 \end{vmatrix} = \frac{1}{2-p}.$$

Pro $p = 0$ a $p = 2$ musíme řešit soustavu individuálně.

$$p=0: \quad \left(\begin{array}{ccc|c} 1 & 0 & 1 & 1\\ 1 & 2 & 1 & -1\\ 0 & 1 & 0 & -1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 1 & 1\\ 0 & 1 & 0 & -1 \end{array}\right),$$

při $z = t$, vychází $y = -1$, $x = 1 - t$,
tj. $(x,y,z) = (1-t, -1, t) = (1,-1,0) + t(-1,0,1)$,
množina řešení: $M = (1,-1,0) + \big\langle(-1,0,1)\big\rangle$.

$$p=2: \quad \left(\begin{array}{ccc|c} 1 & 2 & 1 & 1\\ 1 & 2 & 1 & -1\\ 0 & 1 & 2 & -1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 1 & 1\\ 0 & 0 & 0 & -1 \end{array}\right),$$

podle Frobeniovy věty soustava pro $p = 2$ nemá řešení.

Dodatky k řešení soustav

5.33. Poznámka. Existuje ještě jeden přístup, jak lze hledat bázi prostoru řešení homogenní soustavy. Tento přístup se může hodit při strojovém zpracování a opírá se o následující větu.

5.34. Věta. Nechť homogenní soustava lineárních rovnic $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$ má matici soustavy ve tvaru

$$\mathbf{A} = (\mathbf{E}|\mathbf{C}),$$

kde $\mathbf{E}$ je jednotková matice typu (m, m) a $\mathbf{C}$ je libovolná matice typu (m, k). Pak existuje báze řešení této soustavy $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$, která má tvar:

$$\begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \\ \vdots \\ \boldsymbol{b}_k \end{pmatrix} = (-\mathbf{C}^T|\mathbf{E}'),$$

kde $\mathbf{E}'$ je jednotková matice typu (k, k).

Důkaz. Nejprve překontrolujeme rozměry matic. Nechť počet neznámých soustavy je n, takže matice soustavy $\mathbf{A}$ je typu (m, n). Počet sloupců n této matice se skládá z m sloupců (matice $\mathbf{E}$) a k sloupců (matice $\mathbf{C}$). Je tedy $n = m + k$. Dimenze prostoru řešení je podle věty 5.14 rovna počtu neznámých minus hod $\mathbf{A}$, což je $n - m = k$. To sedí. Skutečně matice $\mathbf{B} = (-\mathbf{C}^T|\mathbf{E}')$ má k řádků a tyto jsou lineárně nezávislé (díky matici $\mathbf{E}'$). Matice $\mathbf{B}$ tedy může obsahovat řádky báze prostoru řešení. Stačí jen ověřit, že každý řádek matice $\mathbf{B}$ řeší soustavu $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$. Tj. stačí ověřit, že $\mathbf{A} \cdot \mathbf{B}^T = \mathbf{O}$, kde $\mathbf{O}$ je nulová matice typu (m, k):

$$\mathbf{A} \cdot \mathbf{B}^T = (\mathbf{E}|\mathbf{C}) \cdot \left(\frac{-\mathbf{C}}{\mathbf{E}'} \right) = \mathbf{E} \cdot (-\mathbf{C}) + \mathbf{C} \cdot \mathbf{E}' = -\mathbf{C} + \mathbf{C} = \mathbf{O}.$$

5.35. Poznámka. Tato věta nám umožňuje rovnou napsat bázi řešení homogenní soustavy, pokud je matice soustavy v uvedeném tvaru. Dokonce, pokud matice soustavy není v uvedeném tvaru, je někdy možné jí eliminací do tohoto tvaru převést, tj. ekvivalentní soustava může mít tento tvar. Pokud ani ekvivalentní soustava nemá tento tvar, dá se prohozením pořadí neznámých dospět k požadovanému tvaru matice soustavy. V takovém případě je ovšem nutné před zapsáním báze prostoru řešení prohodit sloupce matice $\mathbf{B} = (-\mathbf{C}^T|\mathbf{E}')$ zpět. Místo dlouhého vysvětlování ukážeme použití věty na našem příkladu 5.23, ovšem budeme řešit jen přidruženou homogenní soustavu.

5.36. Příklad. Najdeme bázi prostoru řešení soustavy z příkladu 5.11. Eliminujeme matici soustavy:

$$\begin{pmatrix} 1 & 1 & 2 & 3 & 3 & 3 \\ 1 & 1 & 1 & 3 & 1 & 1 \\ 2 & 2 & 2 & 6 & 2 & 8 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 3 & 3 & 3 \\ 0 & 0 & -1 & 0 & -2 & -2 \\ 0 & 0 & -2 & 0 & -4 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 3 & 3 & 3 \\ 0 & 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 3 & 3 & 3 \\ 0 & 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Eliminujeme dále zpětným chodem, abychom ve sloupcích 1, 3 a 6 dostali jednotkové vektory:

$$\begin{pmatrix} 1 & 1 & 2 & 3 & 3 & 3 \\ 0 & 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 3 & 3 & 0 \\ 0 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 3 & -1 & 0 \\ 0 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Prohodíme druhý sloupec s třetím a poslední sloupec s novým třetím (měníme pořadí proměnných)

$$\begin{pmatrix} 1 & 0 & 0 & 3 & -1 & 1 \\ 0 & 1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

a dostáváme matici podle předpokladu věty 5.34. Bázi řešení soustavy s takovou maticí můžeme podle této věty zapsat do matice, kde každý řádek obsahuje jeden bázický vektor:

$$\begin{pmatrix} -3 & 0 & 0 & 1 & 0 & 0 \\ 1 & -2 & 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Zpětně přehodíme poslední sloupec s třetím a druhý s novým třetím a dostáváme matici, obsahující (po řádcích) bázi řešení původní soustavy

$$\begin{pmatrix} -3 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & -2 & 0 & 1 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

5.37. Poznámka. Doc. Krajník ve svých skriptech o maticích [14] hned z kraje uvádí jednoduchý postřeh, který, když si uvědomíme, můžeme mít život s lineární algebrou snadnější. *Násobíme-li matice* $\mathbf{A} \cdot \mathbf{X} = \mathbf{B}$*, pak sloupce matice* $\mathbf{B}$ *obsahují výsledky násobení* $\mathbf{A} \cdot$ *odpovídající sloupec matice* $\mathbf{X}$. *Soustava lineárních soustav*

Uvažujme maticovou rovnost $\mathbf{AX} = \mathbf{B}$, ve které jsou dány matice $\mathbf{A}$ a $\mathbf{B}$ a hledáme matici $\mathbf{X}$. Označme $\mathbf{B} = (\boldsymbol{b}_1^T, \dots, \boldsymbol{b}_k^T)$, tj. matice má k sloupců. Stejný počet sloupců musí mít matice $\mathbf{X}$ (jinak by rovnost nemohla platit), takže $\mathbf{X} = (\boldsymbol{x}_1^T, \dots \boldsymbol{x}_k^T)$. Hledání matice $\mathbf{X}$ pak přechází v hledání jejích sloupců $\boldsymbol{x}_1, \dots, \boldsymbol{x}_k$ tak, že musejí být splněny současně tyto soustavy nehomogenních lineárních rovnic:

$$\mathbf{A} \cdot \boldsymbol{x}_1^T = \boldsymbol{b}_1^T, \quad \mathbf{A} \cdot \boldsymbol{x}_2^T = \boldsymbol{b}_2^T, \quad \dots, \quad \mathbf{A} \cdot \boldsymbol{x}_k^T = \boldsymbol{b}_k^T.$$

Všechny tyto soustavy mají stejnou matici soustavy a jejich rozšířené matice soustav je možné eliminovat společně:

$$(\mathbf{A}|\mathbf{B}) \sim (\mathbf{A}_1|\mathbf{B}_1).$$

Tyto dvě soustavy soustav $\mathbf{AX} = \mathbf{B}$ a $\mathbf{A}_1\mathbf{X} = \mathbf{B}_1$ jsou ekvivalentní, tj. mají stejnou množinu řešení, protože matice jedné soustavy vznikla z matice druhé soustavy eliminací. Všechny soustavy mají společnou přidruženou homogenní soustavu, takže její množinu řešení je možné hledat jen jednou. K jednotlivým vektorům pravých stran pak hledáme jen odpovídající partikulární řešení.

5.38. Příklad. Řešme maticovou rovnost

$$\begin{pmatrix} 1 & 1 & 2 & 3 & 3 & 3 \\ 1 & 1 & 1 & 3 & 1 & 1 \\ 2 & 2 & 2 & 6 & 2 & 8 \end{pmatrix} \cdot \mathbf{X} = \begin{pmatrix} 2 & 4 & 3 & 3 \\ 2 & 2 & 1 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

Soustavu soustav řešíme eliminací:

$$\left(\begin{array}{cccccc|cccc} 1 & 1 & 2 & 3 & 3 & 3 & 2 & 4 & 3 & 3 \\ 1 & 1 & 1 & 3 & 1 & 1 & 2 & 2 & 1 & 3 \\ 2 & 2 & 2 & 6 & 2 & 8 & 1 & 2 & 3 & 4 \end{array}\right) \sim \left(\begin{array}{cccccc|cccc} 1 & 1 & 2 & 3 & 3 & 3 & 2 & 4 & 3 & 3 \\ 0 & 0 & 1 & 0 & 2 & 2 & 0 & 2 & 2 & 0 \\ 0 & 0 & 2 & 0 & 4 & -2 & 3 & 6 & 3 & 2 \end{array}\right) \sim \left(\begin{array}{cccccc|cccc} 1 & 1 & 2 & 3 & 3 & 3 & 2 & 4 & 3 & 3 \\ 0 & 0 & 1 & 0 & 2 & 2 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 6 & -3 & -2 & 1 & -2 \end{array}\right).$$

Přidruženou homogenní soustavu známe už z předchozích příkladů, takže víme, že její prostor řešení má bázi $\{(-1,1,0,0,0,0), (-3,0,0,1,0,0), (1,0,-2,0,1,0)\}$. Partikulární řešení budeme hledat pro každý sloupec pravých stran zvlášť. Počítat budeme poslední, třetí a první složku, v ostatních předpokládáme nuly. Pro sloupec $(2,0,-3)^T$ máme řešení $(\frac{3}{2}, 0, 1, 0, 0, -\frac{1}{2})$, pro sloupec $(4,2,-2)^T$ máme řešení $(-\frac{1}{3}, 0, \frac{8}{3}, 0, 0, -\frac{1}{3})$, pro sloupec $(3,2,1)^T$ máme řešení $(-\frac{5}{6}, 0, \frac{5}{3}, 0, 0, \frac{1}{6})$ a konečně pro sloupec $(3,0,-2)^T$ máme řešení $(\frac{8}{3}, 0, \frac{2}{3}, 0, 0, -\frac{1}{3})$. Zapíšeme-li tato řešení do sloupců vedle sebe, máme jedno z možných řešení pro hledanou matici $\mathbf{X}$. Když k této matici přičteme matici, která bude mít čtyři stejné sloupce tvaru $\alpha\,(-1,1,0,0,0,0)^T + \beta\,(-3,0,0,1,0,0)^T + \gamma\,(1,0,-2,0,1,0)^T$, $\alpha, \beta, \gamma \in \mathbf{R}$, dostáváme zápis obecně všech matic $\mathbf{X}$, které vyhovují zadané maticové rovnici.

5.39. Věta. Nechť $\mathbf{A}$ je regulární matice a $\mathbf{B}$ je libovolná matice se stejným počtem řádků. Rovnost $\mathbf{A} \cdot \mathbf{X} = \mathbf{B}$ je ekvivalentní s $(\mathbf{A}|\mathbf{B}) \sim (\mathbf{E}|\mathbf{X})$.

Důkaz. Protože $\mathbf{A}$ je regulární, má soustava soustav $\mathbf{AX} = \mathbf{B}$ jediné řešení. Eliminujme rozšířenou matici této soustavy soustav:

$$(\mathbf{A}|\mathbf{B}) \sim (\mathbf{E}|\mathbf{X}).$$

Rozšířená matice $(\mathbf{E}|\mathbf{X})$ obsahuje vpravo od čáry řešení původní soustavy soustav $\mathbf{AX} = \mathbf{B}$ právě tehdy, když $(\mathbf{E}|\mathbf{X})$ vznikla eliminací z původní rozšířené matice $(\mathbf{A}|\mathbf{B})$.

5.40. Poznámka. Podobným postupem můžeme snadno obhájit známou metodu výpočtu inverzní matice $(\mathbf{A}|\mathbf{E}) \sim (\mathbf{E}|\mathbf{A}^{-1})$. Vpravo od $\mathbf{E}$ máme řešení soustavy soustav $\mathbf{AX} = \mathbf{E}$, tj. máme tam inverzní matici.

5.41. Poznámka. Maticovou rovnici $\mathbf{XA} = \mathbf{B}$ (při daných maticích $\mathbf{A}$, $\mathbf{B}$) bychom řešili například tak, že transponujeme obě strany rovnosti. Tím dostáváme $\mathbf{A}^T \cdot \mathbf{X}^T = \mathbf{B}^T$ a problém je převeden na tvar, se kterým už si víme rady.

5.42. Poznámka. Důkaz věty 6.31 (v následující kapitole) lze přeformulovat pomocí zde uvedené myšlenky soustavy soustav. To si dovolím přenechat čtenáři. Je to velmi názorné.

6. Více o lineárních prostorech konečné dimenze

6.1. Poznámka. V některých učebnicích, např. [7], se lineárním prostorům konečné dimenze říká *vektorové prostory.* V jiných učebnicích, např. [5], se pod pojmem vektorový prostor myslí obecný lineární prostor třeba i nekonečné dimenze. Vzhledem k této terminologické nejednotě nebudeme vůbec pojem vektorový prostor používat a budeme raději zdlouhavě mluvit o lineárních prostorech konečné dimenze.

6.2. Poznámka. Hlavním cílem této kapitoly je definice pojmu souřadnice vektoru vzhledem k bázi a pojem matice přechodu. Než se do toho pustíme, zmíníme ještě jednu větu o dimenzi průniku a sjednocení podprostorů. Věta 1.22 nám říká, že sjednocení dvou podprostorů nemusí být lineární prostor. Je proto výhodné formulovat následující definici.

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

6.4. Poznámka. Podle věty 2.38 je $M \vee N$ nejmenší podprostor, který obsahuje všechny prvky z M i N dohromady.

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

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

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

Je-li $\boldsymbol{x} \in M \vee N = \langle M \cup N \rangle$, pak podle definice lineárního obalu existuje konečně mnoho prvků z M a konečně mnoho prvků z N takových, že $\boldsymbol{x}$ je lineární kombinací těchto prvků. Tuto lineární kombinaci rozdělíme na součet násobků prvků z M a součet násobků ostatních prvků (tedy prvků z N). První součet označíme $\boldsymbol{y}$ a druhý $\boldsymbol{z}$. Protože M a N jsou podprostory, je podle věty 2.37 $\langle M \rangle = M$, $\langle N \rangle = N$, takže lineární kombinace prvků z M leží v M a podobně pro N. Máme tedy $\boldsymbol{y} \in M$, $\boldsymbol{z} \in N$. Protože $\boldsymbol{x} = \boldsymbol{y} + \boldsymbol{z}$, je $\boldsymbol{x} \in \{\boldsymbol{y} + \boldsymbol{z};\ \boldsymbol{y} \in M, \boldsymbol{z} \in N\}$. To dokazuje obrácenou inkluzi.

6.6. Věta. Nechť L je lineární prostor konečné dimenze, M a N jsou jeho podprostory. Pak *Dimenze průniku a spojení*

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

Důkaz (pro hloubavé čtenáře). Nechť $\dim M = m$, $\dim N = n$, $\dim(M \cap N) = k$. Nechť $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$ je báze podprostoru $M \cap N$. Vzhledem k tomu, že $M \cap N \subseteq M$, lze lineárně nezávislé vektory $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$ doplnit o další prvky, aby dohromady tvořily bázi v M. Viz větu 2.51. Podobně lze doplnit $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$ o další prvky, aby tvořily bázi v N. Máme tedy

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

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

Ukážeme nejdříve, že $\langle B \rangle = M \vee N$. Protože $B \subseteq M \cup N$, je $\langle B \rangle \subseteq \langle M \cup N \rangle = M \vee N$. Nyní ukážeme obrácenou inkluzi. Je-li $\boldsymbol{x} \in M \vee N$, pak podle věty 6.5 existují vektory $\boldsymbol{y} \in M$ a $\boldsymbol{z} \in N$ takové, že $\boldsymbol{x} = \boldsymbol{y} + \boldsymbol{z}$. Vektor $\boldsymbol{y}$ lze zapsat jako lineární kombinaci prvků báze M a vektor $\boldsymbol{z}$ jako lineární kombinaci prvků báze N. Proto je vektor $\boldsymbol{x}$ lineární kombinací prvků množiny B a máme dokázánu obrácenou inkluzi $M \vee N \subseteq \langle B \rangle$.

Nyní ukážeme, že B je lineárně nezávislá množina. Množina $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k, \boldsymbol{c}_{k+1}, \ldots, \boldsymbol{c}_m\}$ je lineárně nezávislá, protože je bází prostoru M. Množina $\{\boldsymbol{d}_{k+1}, \ldots, \boldsymbol{d}_n\}$ je také lineárně nezávislá, protože je podmnožinou báze prostoru N. Navíc pro všechny prvky $\boldsymbol{d}_i$, $i \in \{k+1, \ldots, n\}$ platí, že neleží v M, tedy $\boldsymbol{d}_i \notin \langle \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k, \boldsymbol{c}_{k+1}, \ldots, \boldsymbol{c}_m \rangle$. Přidáním těchto prvků k vektorům $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k, \boldsymbol{c}_{k+1}, \ldots, \boldsymbol{c}_m$ zůstává rozšířená množina podle věty 2.39 lineárně nezávislá.

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

6.7. Příklad. Jsou dány lineární podprostory M a N lineárního prostoru $\mathbf{R}^5$ pomocí lineárních obalů:

$$M = \big\langle (1,2,0,1,1),(1,3,1,3,4),(3,5,2,4,5)\big\rangle,$$
$$N = \big\langle (1,1,3,4,3),(1,0,2,2,0),(2,1,3,2,3),(0,1,2,4,3)\big\rangle.$$

Najdeme bázi a dimenzi prostorů M, N, $M\cap N$ a $M\vee N$.

Podle věty 3.13 zachovává Gaussova eliminační metoda lineární obal řádků matice, takže budeme eliminovat následující matice:

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

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

Podle věty 3.22 jsou řádky matic zapsaných nejvíce vpravo lineárně nezávislé. Lineární obal těchto řádků zůstal zachován a je roven M, respektive N. Máme 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 lineárně nezávislé, můžeme zapsat i jinou bázi M: $\{(1,2,0,1,1),(1,3,1,3,4),(3,5,2,4,5)\}$. Vektory, kterými je zadán podprostor N jsou lineárně závislé, takže netvoří bázi.

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

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

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

Podle věty 6.6 máme okamžitě dimenzi průniku:

$$\dim(M\cap N) = \dim M + \dim N - \dim(M\vee N) = 3+3-4 = 2,$$

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

$$\alpha\,(1,2,0,1,1) + \beta\,(0,1,1,2,3) + \gamma\,(0,0,3,3,5) = a\,(1,1,3,4,3) + b\,(0,1,1,2,3) + c\,(0,0,1,2,0). \qquad (6.1)$$

Z tohoto požadavku nám vychází soustava pěti rovnic o šesti neznámých $\alpha,\beta,\gamma,a,b,c$. Eliminujeme matici této homogenní soustavy.

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

Volíme $b=t$, $c=u$, pak vychází $a=-u$. Ostatní hodnoty proměnných nemusíme počítat a vrátíme se k pravé straně rovnosti (6.1). Vektory, které jsou společné oběma prostorům, musejí tedy splňovat:

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

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

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

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

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

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

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

$$\boldsymbol{x} = (\alpha_1, \alpha_2, \ldots, \alpha_n)_{(B)}.$$

6.11. Poznámka. Nechť B je báze lineárního prostoru L. Protože $\langle B \rangle = L$, je každý prvek $\boldsymbol{x}$ lineární kombinací prvků báze a tudíž každý prvek $\boldsymbol{x}$ má nějaké souřadnice vzhledem k uspořádané bázi (B). Následující věta ukazuje, že jsou tyto souřadnice určeny uspořádanou bází (B) jednoznačně. *Existence a jednoznačnost souřadnic*

6.12. Věta. Nechť (B) je uspořádaná báze lineárního porostoru L. Pak pro každý prvek $\boldsymbol{x} \in L$ jsou souřadnice $\boldsymbol{x}$ vzhledem k bázi (B) určeny jednoznačně.

Důkaz. Označme $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$. Nechť $\boldsymbol{x} = (\alpha_1, \alpha_2, \ldots, \alpha_n)_{(B)} = (\beta_1, \beta_2, \ldots, \beta_n)_{(B)}$. Ukážeme, že pak je $\alpha_i = \beta_i$, $\forall i \in \{1, \ldots, n\}$. Podle definice 6.10 je

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

Odečtením těchto rovností dostáváme

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

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

6.13. Věta. Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je uspořádaná báze lineárního prostoru L. Pak pro každý prvek $\boldsymbol{a} \in \mathbf{R}^n$, $\boldsymbol{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, existuje $\boldsymbol{x} \in L$ takový, že $\boldsymbol{x} = (\alpha_1, \alpha_2, \ldots, \alpha_n)_{(B)}$.

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

6.14. Poznámka. Nechť L je blíže neurčený lineární prostor, $\dim L = n$. Souřadnice vektoru vzhledem k uspořádané bázi nám podle právě dokázaných vět umožňuje jednoznačně podchytit každý vektor $\boldsymbol{x} \in L$ pomocí uspořádané n-tice reálných čísel. Přesněji, při pevně volené uspořádané bázi (B) existuje ke každému prvku $\boldsymbol{x} \in L$ jednoznačně určená uspořádaná n-tice $\boldsymbol{a} \in \mathbf{R}^n$, která tvoří souřadnice tohoto vektoru vzhledem k bázi (B) a naopak.

Význam pojmu souřadnice vzhledem k bázi je tedy v tom, že stačí v libovolném lineárním prostoru konečné dimenze (například polynomů nejvýše k-tého stupně, matic, ...) stanovit jednu uspořádanou bázi a pak popsat každý takový prvek uspořádanou n-ticí reálných čísel.

V následující kapitole o lineárních zobrazeních ukážeme, že zobrazení z L na $\mathbf{R}^n$, které přiřazuje každému prvku z L jeho souřadnice vzhledem k pevně zvolené uspořádané bázi, je tzv. izomorfismus. To znamená, že veškeré vlastnosti linearity (součty, násobky, lineární závislosti a nezávislosti, podprostory, lineární obaly atd.) se tímto zobrazením „přenášejí“ z prostoru L na důvěrně známý lineární prostor $\mathbf{R}^n$. Stačí tedy tyto vlastnosti studovat v $\mathbf{R}^n$ a výsledky případně „zpětně přenést“ pomocí inverzního zobrazení do L.

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

Nevěřící Tomášové by nejprve měli ověřit, zda je B skutečně bází lineárního prostoru L, tj. zda platí vlastnosti (1) a (2) z definice 2.42. Položili by následující lineární kombinaci rovnu nulovému polynomu:

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

a zkoumali by, za jakých okolností lze rovnost splnit. Polynom je nulový jen tehdy, když jsou nulové všechny jeho koeficienty, což vede na homogenní soustavu čtyř rovnic o neznámých $\alpha, \beta, \gamma, \delta$. Tu by Tomášové vyřešili, zjistili by, že má pouze nulové řešení, a proto jsou dané polynomy z množiny B lineárně nezávislé. Dále by Tomášové použili vlastnost (3) věty 2.64 a prohlásili, že když množina B je lineárně nezávislá a obsahuje stejný počet vektorů, jako je dimenze prostoru (podle příkladu 2.48 je $\dim L = 4$), pak musí $\langle B\rangle = L$. Tím by zjistili, že B je báze lineárního prostoru L.

Nyní najdeme souřadnice polynomu p vzhledem k bázi (B). Podle definice 6.10 má pro souřadnice $(\alpha, \beta, \gamma, \delta)$ platit

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

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

Po porovnání jednotlivých koeficientů u polynomů na levé a pravé straně rovnosti dostáváme soustavu rovnic

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

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

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

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

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

6.17. Poznámka. Předchozí dva příklady ilustrují skutečnost, že souřadnice vektoru vzhledem k uspořádané bázi jsou závislé na volbě uspořádané báze. Budeme se setkávat s úlohou, kdy jsou dány dvě různé uspořádané báze stejného lineárního prostoru a budeme znát souřadnice nějakého vektoru vzhledem k jedné bázi. Bude potřeba najít souřadnice téhož vektoru vzhledem ke druhé bázi. K tomu slouží tzv. matice přechodu.

Matice přechodu

6.18. Definice. Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ a $(C) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n)$ jsou dvě uspořádané báze stejného lineárního prostoru L. Matici $\mathbf{A}$, která splňuje maticovou rovnost

$$(\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n) \cdot \mathbf{A} = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n) \tag{6.2}$$

nazýváme *maticí přechodu od uspořádané báze* (B) *k uspořádané bázi* (C). Na definiční rovnost (6.2) se díváme jako na součin jednořádkové matice vektorů $(\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ s maticí $\mathbf{A}$ reálných čísel typu (n, n), který se má rovnat jednořádkové matici vektorů $(\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n)$.

Matici přechodu od báze (B) k bázi (C) budeme často pro názornost označovat $\mathbf{A}_{(B,C)}$.

6.19. Věta. Pro každé dvě uspořádané báze stejného lineárního prostoru (B) a (C) existuje právě jedna regulární matice přechodu $\mathbf{A}_{(B,C)}$.

Důkaz. Podle definice maticového součinu a podle (6.2) je

$$\boldsymbol{c}_1 = a_{1,1}\,\boldsymbol{b}_1 + a_{2,1}\,\boldsymbol{b}_2 + \cdots + a_{n,1}\,\boldsymbol{b}_n,$$

kde $a_{1,1}, a_{2,1}, \ldots, a_{n,1}$ jsou prvky prvního sloupce matice $\mathbf{A}_{(B,C)}$. První sloupec matice tedy obsahuje souřadnice vektoru $\boldsymbol{c}_1$ vzhledem k bázi (B). Podobná vlastnost platí pro ostatní vektory $\boldsymbol{c}_i$, tedy i-tý sloupec matice $\mathbf{A}_{(B,C)}$ obsahuje souřadnice vektoru $\boldsymbol{c}_i$ vzhledem k bázi (B). To je návod, jak sestrojit hledanou matici. Matice tedy existuje a sloupce této matice jsou podle věty 6.12 určeny jednoznačně.

Ukážeme ještě, že matice $\mathbf{A}_{(B,C)}$ je regulární matice. Sloupce této matice musejí být lineárně nezávislé, protože tyto sloupce jsou násobeny stejnou jednořádkovou maticí $(\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$, a přitom tímto násobením mají vzniknout lineárně nezávislé vektory $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n$. Protože jsou sloupce matice $\mathbf{A}_{(B,C)}$ lineárně nezávislé, tj. $\operatorname{hod} \mathbf{A}^T_{(B,C)} = \operatorname{hod} \mathbf{A}_{(B,C)} = n$, je matice přechodu regulární.

6.20. Poznámka. Transponujeme-li obě strany rovnosti (6.2), dostáváme maticovou rovnost

$$\mathbf{A}^T_{(B,C)} \cdot \begin{pmatrix} \boldsymbol{b}_1 \\ \vdots \\ \boldsymbol{b}_n \end{pmatrix} = \begin{pmatrix} \boldsymbol{c}_1 \\ \vdots \\ \boldsymbol{c}_n \end{pmatrix},$$

se kterou se můžeme setkat v některých učebnicích jako definiční rovností pro matici přechodu. Všimněme si, že se zde pracuje s maticí transponovanou k matici přechodu. Někteří autoři proto definují místo matice přechodu podle definice 6.18 matici k ní transponovanou.

6.21. Věta. Je-li $\mathbf{A}$ matice přechodu od báze (B) k bázi (C), pak $\mathbf{A}^{-1}$ je matice přechodu od báze (C) k bázi (B).

Důkaz. Plyne rovnou vynásobením rovnosti (6.2) maticí $\mathbf{A}^{-1}$ zprava.

6.22. Příklad. Nechť L je lineární prostor polynomů z příkladů 6.15 a 6.16. Připomeňme uspořádané báze z těchto příkladů: $(B) = \big(x+1, x-1, (x+1)^2, (x+1)^3\big)$, $(B_0) = (1, x, x^2, x^3)$. Pak jsme schopni podle definice 6.18 rovnou zapsat jednotlivé sloupce matice přechodu od báze (B_0) k bázi (B):

$$(1, x, x^2, x^3) \cdot \begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \big(x+1, x-1, (x+1)^2, (x+1)^3\big).$$

Pokud bychom chtěli najít matici přechodu od báze (B) k bázi (B_0), není přímé zapsání složek jednotlivých sloupců tak jednoduché. Použijeme proto větu 6.21 a budeme počítat inverzní matici k právě sestrojené matici:

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

Zapíšeme ještě jednou obě matice přechodu od báze (B_0) k (B) a od báze (B) k (B_0):

$$\mathbf{A}_{(B_0,B)} = \begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \mathbf{A}_{(B,B_0)} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & -\frac{3}{2} & \frac{5}{2} \\ -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

6.23. Věta. Nechť (B) a (C) jsou dvě uspořádané báze lineárního prostoru L, $\mathbf{A}_{(B,C)}$ je matice přechodu od (B) k (C). Pak pro souřadnice každého vektoru $\boldsymbol{x} \in L$, $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)_{(B)} = (y_1, y_2, \ldots, y_n)_{(C)}$ platí

Souřadnice vektoru a matice přechodu

$$\mathbf{A}_{(B,C)} \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}. \tag{6.3}$$

Důkaz. Věta je důsledkem věty o maticích lineárního zobrazení. Důkaz proto odložíme do následující kapitoly. Viz poznámku 7.58 v kapitole o lineárních zobrazeních.

6.24. Poznámka. Vzorec (6.3) si lze pamatovat takto:

$$\mathbf{A}_{(B,C)} \cdot \begin{pmatrix} \text{souřadnice} \\ \text{vzhledem} \\ \text{k bázi } (C) \end{pmatrix} = \begin{pmatrix} \text{souřadnice} \\ \text{vzhledem} \\ \text{k bázi } (B) \end{pmatrix}.$$

Vidíme, že matice přechodu od (B) k (C) umožňuje počítat maticovým násobením souřadnice vzhledem k bázi (B), pokud známe souřadnice vzhledem k bázi (C). Matice přechodu tedy převádí souřadnice přesně obráceně, než by vyplývalo z jejího názvu.

6.25. Příklad. Vraťme se k bázím $(B) = \big(x+1, x-1, (x+1)^2, (x+1)^3\big)$ a $(B_0) = (1, x, x^2, x^3)$ z předchozího příkladu. Polynom $p \in L$, $p(x) = 2x^3 + x^2 - 3x$ má podle příkladu 6.16 souřadnice $p = (0, -3, 1, 2)_{(B_0)}$. Uvažujme ještě polynom $q \in L$ daný vzorcem $q(x) = x^2 + 5$, $\forall x \in \mathbf{R}$. Polynom q má tedy souřadnice $q = (5, 0, 1, 0)_{(B_0)}$.

Za použití matice přechodu najdeme souřadnice polynomů p a q vzhledem k bázi (B).

Matici přechodu $\mathbf{A}_{(B,B_0)}$ jsme spočítali v příkladu 6.22. Nyní použijeme vzorec (6.3):

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & -\frac{3}{2} & \frac{5}{2} \\ -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ -3 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \\ -5 \\ 2 \end{pmatrix}, \qquad \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & -\frac{3}{2} & \frac{5}{2} \\ -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ -3 \\ 1 \\ 0 \end{pmatrix}.$$

Máme tedy výsledek: $p = (2, -1, -5, 2)_{(B)}, q = (1, -3, 1, 0)_{(B)}$.

6.26. Poznámka. Všimneme si, že jsme souřadnice polynomu p vzhledem k bázi (B) spočítali už v příkladu 6.15 bez použití matice přechodu. Stačilo nám rozepsat definici souřadnic vzhledem k bázi.

Pokud potřebujeme zjistit souřadnice jediného vektoru vzhledem k nějaké bázi, pak je zřejmě účelnější použít definici pojmu souřadnice vzhledem k bázi a maticemi přechodu si zbytečně nekomplikovat život. Jakmile ale budeme potřebovat převádět souřadnice většího množství vektorů, pak se vyplatí najít odpovídající matici přechodu.

V příkladu 6.15 jsme vlastně nevědomky použili matici přechodu $\mathbf{A}_{(B_0,B)}$. Byla to matice soustavy lineárních rovnic, pro kterou jsme hledali řešení.

6.27. Věta. Nechť $\mathbf{A}_{(B,C)}$ je matice přechodu od báze (B) k bázi (C) a $\mathbf{A}_{(C,D)}$ je matice přechodu od báze (C) k bázi (D). Pak pro matici přechodu $\mathbf{A}_{(B,D)}$ od báze (B) k bázi (D) platí

Přechod od báze (B) přes (C) k (D)

$$\mathbf{A}_{(B,D)} = \mathbf{A}_{(B,C)} \cdot \mathbf{A}_{(C,D)}.$$

Důkaz. Podle definice matice přechodu 6.18 je $(B) \cdot \mathbf{A}_{(B,C)} = (C)$, $(C) \cdot \mathbf{A}_{(C,D)} = (D)$. Vynásobíme-li první rovnost maticí $\mathbf{A}_{(C,D)}$ zprava, dostáváme

$$(B) \cdot \mathbf{A}_{(B,C)} \cdot \mathbf{A}_{(C,D)} = (C) \cdot \mathbf{A}_{(C,D)} = (D).$$

6.28. Poznámka. Na závěr této kapitoly se pokusíme ukázat metodu, jak sestavit matici přechodu, jsou-li dány uspořádané báze (B) a (C) v $\mathbf{R}^n$. Nejprve si všimneme, jaká je souvislost mezi složkami vektorů z $\mathbf{R}^n$ a jejich souřadnicemi.

Sestavení matic přechodu

6.29. Věta. Nechť $\boldsymbol{a} \in \mathbf{R}^n$, $\boldsymbol{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Složky $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ jsou souřadnicemi vektoru $\boldsymbol{a}$ vzhledem ke standardní bázi (S):

$$(S) = \big((1,0,0,\ldots,0), (0,1,0,\ldots,0), \ldots, (0,0,0,\ldots,1)\big).$$

Důkaz. Pro vektor $\boldsymbol{a} \in \mathbf{R}^n$ platí

$$\boldsymbol{a} = \alpha_1\,(1,0,0,\ldots,0) + \alpha_2\,(0,1,0,\ldots,0) + \cdots + \alpha_n\,(0,0,0,\ldots,1).$$

V souladu s definicí 6.10 jsou tedy složky $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ souřadnicemi vektoru $\boldsymbol{a}$ vzhledem k bázi (S).

6.30. Věta. Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je uspořádaná báze lineárního prostoru $\mathbf{R}^n$. Matice přechodu od standardní báze (S) k bázi (B) má tvar

$$\mathbf{A}_{(S,B)} = (\boldsymbol{b}_1^T, \boldsymbol{b}_2^T, \ldots, \boldsymbol{b}_n^T),$$

kde symbolem $\boldsymbol{b}_i^T$ značíme sloupec složek vektoru $\boldsymbol{b}_i$. Jinými slovy, uvedenou matici přechodu sestavíme tak, že zapíšeme jednotlivé vektory báze vedle sebe, složky těchto vektorů zapíšeme do sloupců.

Důkaz. Stačí si zopakovat důkaz věty 6.19. Vidíme, že i-tý sloupec matice $\mathbf{A}_{(S,B)}$ podle tohoto důkazu obsahuje souřadnice vektoru $\boldsymbol{b}_i$ vzhledem k bázi (S). Podle věty 6.29 jsou tyto souřadnice rovny přímo složkám vektoru $\boldsymbol{b}_i$.

6.31. Věta. Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ a $(C) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n)$ jsou uspořádané báze lineárního prostoru $\mathbf{R}^n$. Pak pro matice přechodu $\mathbf{A}_{(B,C)}$ a $\mathbf{A}_{(C,B)}$ platí

$$(\mathbf{A}_{(C,B)} \,|\, \mathbf{E}) \sim (\boldsymbol{b}_1^T, \boldsymbol{b}_2^T, \ldots \boldsymbol{b}_n^T \,|\, \boldsymbol{c}_1^T, \boldsymbol{c}_2^T, \ldots \boldsymbol{c}_n^T) \sim (\mathbf{E} \,|\, \mathbf{A}_{(B,C)}),$$

kde „$\sim$“ značí konečně mnoho kroků Gaussovy eliminační metody, $\mathbf{E}$ je jednotková matice a $\boldsymbol{b}_i^T$ resp. $\boldsymbol{c}_j^T$ jsou vektory $\boldsymbol{b}_i$ resp. $\boldsymbol{c}_j$, jejichž složky jsou zapsány do sloupců.

Důkaz. Podle věty 6.30 je

$$(\boldsymbol{b}_1^T, \boldsymbol{b}_2^T, \ldots \boldsymbol{b}_n^T \,|\, \boldsymbol{c}_1^T, \boldsymbol{c}_2^T, \ldots \boldsymbol{c}_n^T) = (\mathbf{A}_{(S,B)} \,|\, \mathbf{A}_{(S,C)}).$$

Dále podle vět 6.27 a 6.21 je $\mathbf{A}_{(B,C)} = \mathbf{A}_{(B,S)} \cdot \mathbf{A}_{(S,C)} = \mathbf{A}_{(S,B)}^{-1} \cdot \mathbf{A}_{(S,C)}$.

Protože $(\mathbf{A}_{(S,B)} \,|\, \mathbf{A}_{(S,C)}) \sim (\mathbf{E} \,|\, \mathbf{X})$, existuje podle věty 3.55 taková regulární matice $\mathbf{P}$, pro kterou platí $(\mathbf{P} \cdot \mathbf{A}_{(S,B)} \,|\, \mathbf{P} \cdot \mathbf{A}_{(S,C)}) = (\mathbf{E} \,|\, \mathbf{X})$. Z rovnosti $\mathbf{P} \cdot \mathbf{A}_{(S,B)} = \mathbf{E}$ plyne $\mathbf{P} = \mathbf{A}_{(S,B)}^{-1}$. Dostáváme tedy

$$\mathbf{X} = \mathbf{P} \cdot \mathbf{A}_{(S,C)} = \mathbf{A}_{(S,B)}^{-1} \cdot \mathbf{A}_{(S,C)} = \mathbf{A}_{(B,C)}.$$

Skutečnost, že $(\mathbf{A}_{(C,B)} \,|\, \mathbf{E}) \sim (\mathbf{A}_{(S,B)} \,|\, \mathbf{A}_{(S,C)})$ bychom dokázali podobně.

6.32. Poznámka. Věta 6.31 nám dává návod, jak sestavit matici přechodu od báze (B) k bázi (C) v $\mathbf{R}^n$. Stačí zapsat vedle sebe vektory obou bází (jejich složky jsou psány do sloupců) a pak eliminovat tak, abychom získali v levém poli jednotkovou matici. V pravém poli pak máme hledanou matici přechodu.

6.33. Příklad. Jsou dány uspořádané báze (B) a (C) v lineárním prostoru $\mathbf{R}^4$:

$$(B) = \big((1,1,1,1), (1,2,1,1), (1,1,2,1), (1,3,2,3)\big),$$
$$(C) = \big((1,0,3,3), (1,2,1,1), (2,2,5,4), (-2,-3,-4,-4)\big).$$

Najdeme matice přechodu $\mathbf{A}_{(B,C)}$ a $\mathbf{A}_{(C,B)}$. Dále je dán vektor $\boldsymbol{x} \in \mathbf{R}^4$, $\boldsymbol{x} = (0,1,1,0)$. Máme najít jeho souřadnice vzhledem k oběma uspořádaným bázím.

Sestavíme matici vektorů obou bází podle věty 6.31 a budeme ji eliminovat „oběma směry“.

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

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

Je tedy

$$\mathbf{A}_{(B,C)} = \begin{pmatrix} 2&0&1&-1\\ -3&1&-2&1\\ 1&0&2&-1\\ 1&0&1&-1 \end{pmatrix}, \qquad \mathbf{A}_{(C,B)} = \begin{pmatrix} 1&0&0&-1\\ 2&1&1&-2\\ 0&0&1&-1\\ 1&0&1&-3 \end{pmatrix}.$$

Vektor $\boldsymbol{x} = (0,1,1,0)$ má podle definice 6.10 souřadnice $(\alpha, \beta, \gamma, \delta)$ vzhledem k bázi (B), pokud platí

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

To vede na nehomogenní soustavu lineárních rovnic, jejíž rozšířená matice je

$$\left(\begin{array}{cccc|c} 1&1&1&1&0\\ 1&2&1&3&1\\ 1&1&2&2&1\\ 1&1&1&3&0 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1&1&1&1&0\\ 0&1&0&2&1\\ 0&0&1&1&1\\ 0&0&0&1&0 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1&0&0&0&-2\\ 0&1&0&0&1\\ 0&0&1&0&1\\ 0&0&0&1&0 \end{array}\right), \qquad \text{výsledek: } \boldsymbol{x} = (-2,1,1,0)_{(B)}.$$

Pro nalezení souřadnic vektoru $\boldsymbol{x}$ vzhledem k bázi (C) využijeme právě spočítaného výsledku a věty 6.23.

$$\begin{pmatrix} 1&0&0&-1\\ 2&1&1&-2\\ 0&0&1&-1\\ 1&0&1&-3 \end{pmatrix} \cdot \begin{pmatrix} -2\\ 1\\ 1\\ 0 \end{pmatrix} = \begin{pmatrix} -2\\ -2\\ 1\\ -1 \end{pmatrix}, \qquad \text{výsledek: } \boldsymbol{x} = (-2,-2,1,-1)_{(C)}.$$

7. Lineární zobrazení

7.1. Poznámka. Než se pustíme do definice pojmu lineární zobrazení, bude užitečné si zopakovat, co to je vůbec zobrazení a jeho základní vlastnosti.

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

Je-li $\boldsymbol{x} \in L_1$, pak zobrazení $\mathcal{A}\colon L_1 \to L_2$ přiřadí prvku $\boldsymbol{x}$ jednoznačně nějaký prvek z množiny L_2. Tento prvek označujeme symbolem $\mathcal{A}(\boldsymbol{x}) \in L_2$ a říkáme mu *hodnota zobrazení $\mathcal{A}$ v bodě $\boldsymbol{x}$*. Je-li $M \subseteq L_1$, pak definujeme

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

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

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

7.5. Definice. Nechť L_1 a L_2 jsou libovolné množiny a uvažujme $\mathcal{A}\colon L_1 \to L_2$. Zobrazení $\mathcal{A}$ je *prosté* (*injektivní*), pokud pro každé dva prvky $\boldsymbol{x}_1 \in L_1$, $\boldsymbol{x}_2 \in L_1$, $\boldsymbol{x}_1 \neq \boldsymbol{x}_2$ platí $\mathcal{A}(\boldsymbol{x}_1) \neq \mathcal{A}(\boldsymbol{x}_2)$. *Prosté zobrazení*

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

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

7.7. Poznámka. Lineární zobrazení „zachovává“ operace sčítání a násobení konstantou. Sečteme-li dva prvky z L_1 a výsledek převedeme prostřednictvím lineárního zobrazení do L_2, výjde totéž, jako kdybychom nejprve jednotlivé prvky převedli prostřednictvím zobrazení do L_2 a tam je sečetli. Všimneme si, že první operace „+“ ve vlastnosti (1) je sčítáním definovaným na lineárním prostoru L_1, zatímco druhá operace „+“ v této vlastnosti je sčítáním definovaným na lineárním prostoru L_2. Tato dvě sčítání mohou být definována zcela rozdílným způsobem na zcela rozdílných lineárních prostorech. Podobně ve vlastnosti (2) je první operace „·“ násobkem definovaným na L_1, zatímco druhá operace „·“ je násobek definovaný na L_2.

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

$$\mathcal{A}(\alpha\,\boldsymbol{x} + \beta\,\boldsymbol{y}) = \alpha\,\mathcal{A}(\boldsymbol{x}) + \beta\,\mathcal{A}(\boldsymbol{y}). \tag{7.1}$$

Důkaz. Nejprve předpokládejme, že pro zobrazení $\mathcal{A}\colon L_1 \to L_2$ platí (7.1) pro všechna $\boldsymbol{x}, \boldsymbol{y} \in L_1$ a $\alpha, \beta \in \mathbf{R}$. Dokážeme, že $\mathcal{A}$ je lineární, tj. že platí (1) a (2) z definice 7.6. Pokud zvolíme $\alpha = \beta = 1$, plyne z (7.1) vlastnost (1) a pokud volíme $\beta = 0$, plyne z (7.1) vlastnost (2).

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

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

Nad rovnítky jsme uvedli, kterou vlastnost jsme zrovna použili.

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

$$\mathcal{A}(\alpha_1\,\boldsymbol{x}_1 + \alpha_2\,\boldsymbol{x}_2 + \cdots + \alpha_n\,\boldsymbol{x}_n) = \alpha_1\,\mathcal{A}(\boldsymbol{x}_1) + \alpha_2\,\mathcal{A}(\boldsymbol{x}_2) + \cdots + \alpha_n\,\mathcal{A}(\boldsymbol{x}_n). \tag{7.2}$$

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

Důkaz. Podle vlastnosti (7) definice 1.6 je $\boldsymbol{o}_1 = 0\,\boldsymbol{x}$, kde $\boldsymbol{x} \in L_1$. Podle vlastnosti (2) definice 7.6 je $\mathcal{A}(\boldsymbol{o}_1) = \mathcal{A}(0\,\boldsymbol{x}) = 0\,\mathcal{A}(\boldsymbol{x}) = \boldsymbol{o}_2$.

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

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

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

Ověříme vlastnosti (1) a (2) z definice 7.6:

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

7.12. Příklad. Zobrazení $\mathcal{A}\colon \mathbf{R}^4 \to \mathbf{R}^3$ definované předpisem $\mathcal{A}(x_1, x_2, x_3, x_4) = (x_2 + x_3, x_3 + 3, 2x_1)$ není lineární, protože $\mathcal{A}(0, 0, 0, 0) = (0, 3, 0)$ a to není nulový vektor v $\mathbf{R}^3$. Podle věty 7.10 musí každé lineární zobrazení zobrazit nulový vektor na nulový vektor.

Pilnější čtenáři si zkusí ověřit, že $\mathcal{A}$ není lineární, přímo z definice 7.6 nebo z principu superpozice 7.8.

7.13. Příklad. Nechť L_1 je lineární prostor všech diferencovatelných funkcí na $\mathbf{R}$ a L_2 je lineární prostor všech funkcí na $\mathbf{R}$. Pak zobrazení $\mathcal{A}\colon L_1 \to L_2$, které každé funkci z L_1 přiřadí její derivaci, je lineární. Platí totiž

$$\mathcal{A}(f + g) = (f + g)' = f' + g' = \mathcal{A}(f) + \mathcal{A}(g), \qquad \mathcal{A}(\alpha f) = (\alpha f)' = \alpha\,f' = \alpha\,\mathcal{A}(f).$$

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

Důkaz. Nechť $\boldsymbol{y} \in \mathcal{A}\big(\langle M\rangle\big)$. Pak existuje vektor $\boldsymbol{x} \in \langle M\rangle$ takový, že $\mathcal{A}(\boldsymbol{x}) = \boldsymbol{y}$. Protože $\boldsymbol{x} \in \langle M\rangle$, existuje podle definice lineárního obalu konečně mnoho $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_i \in M$ takových, že $\boldsymbol{x}$ je lineární kombinací těchto vektorů. Protože $\mathcal{A}$ je lineární, máme podle (7.2)

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

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

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

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

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

7.15. Poznámka. Věta 7.14 má tento důsledek: Je-li $M \subseteq L_1$ lineární podprostor v L_1, pak $\mathcal{A}(M)$ je lineární podprostor v L_2. Stačí si uvědomit platnost věty 2.37. Lineární zobrazení nám tedy převádí podprostory na podprostory.

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

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

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

7.17. Příklad. Uvažujme zobrazení definované v příkladu 7.13, které každé funkci přiřadí její derivaci. Jádrem tohoto zobrazení je množina všech konstantních funkcí, protože to jsou právě všechny funkce, které po zderivování dávají nulovou funkci.

7.18. Příklad. Najdeme jádro zobrazení $\mathcal{A}$ z příkladu 7.11. Podle definice jádra je

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

To vede na homogenní soustavu tří rovnic o dvou neznámých. V tomto příkladě má tato soustava jen nulové řešení, takže máme

$$\operatorname{Ker}\mathcal{A} = \big\{(0,0)\big\}.$$

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

Důkaz. Především je $\operatorname{Ker}\mathcal{A}$ neprázdná množina, protože podle věty 7.10 obsahuje tato množina nulový vektor. Podle definice 1.17 máme dokázat (1) je-li $\boldsymbol{x} \in \operatorname{Ker}\mathcal{A}$, $\boldsymbol{y} \in \operatorname{Ker}\mathcal{A}$, pak též $\boldsymbol{x}+\boldsymbol{y} \in \operatorname{Ker}\mathcal{A}$ a (2) je-li $\boldsymbol{x} \in \operatorname{Ker}\mathcal{A}$, $\alpha \in \mathbf{R}$, pak je $\alpha\,\boldsymbol{x} \in \operatorname{Ker}\mathcal{A}$. Předpoklady podle definice 7.16 říkají $\mathcal{A}(\boldsymbol{x}) = \mathcal{A}(\boldsymbol{y}) = \boldsymbol{o}_2$ a máme dokázat, že $\mathcal{A}(\boldsymbol{x}+\boldsymbol{y}) = \boldsymbol{o}_2$, $\mathcal{A}(\alpha\,\boldsymbol{x}) = \boldsymbol{o}_2$. Podle definice 7.6 lineárního zobrazení platí

$$\mathcal{A}(\boldsymbol{x}+\boldsymbol{y}) = \mathcal{A}(\boldsymbol{x}) + \mathcal{A}(\boldsymbol{y}) = \boldsymbol{o}_2 + \boldsymbol{o}_2 = \boldsymbol{o}_2, \qquad \mathcal{A}(\alpha\,\boldsymbol{x}) = \alpha\,\mathcal{A}(\boldsymbol{x}) = \alpha\,\boldsymbol{o}_2 = \boldsymbol{o}_2.$$

7.20. Věta. Množina $\mathcal{A}(L_1)$ všech hodnot lineárního zobrazení $\mathcal{A}\colon L_1 \to L_2$ tvoří lineární podprostor lineárního prostoru L_2.

Důkaz. Množina L_1 je sama v sobě podprostorem. Podle věty 7.14 a poznámky 7.15 musí být lineárním podprostorem i množina $\mathcal{A}(L_1)$.

7.21. Definice. *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

Defekt a hodnost zobrazení

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

7.22. Poznámka. Předchozí dvě věty zaručují smysluplnost definice defektu a hodnosti: $\operatorname{Ker}\mathcal{A}$ a $\mathcal{A}(L_1)$ jsou lineární podprostory. Defekt zobrazení udává zhruba řečeno „vzdálenost“ zobrazení od ideálního prostého zobrazení. Jak moc je zobrazení $\mathcal{A}$ „defektní“ souvisí také s tím, kolik informace, které dovedeme v prostoru L_1 rozlišit, se stává po aplikaci zobrazení $\mathcal{A}$ v prostoru L_2 nerozlišitelné.

7.23. Příklad. Defekt zobrazení $\mathcal{A}$ definovaného v příkladu 7.13, které přiřazuje derivaci, je roven jedné. Je totiž množina konstantních funkcí lineárním podprostorem množiny všech funkcí, přitom báze tohoto podprostoru je libovolná jedna nenulová konstantní funkce. Proto je dimenze tohoto podprostoru rovna jedné.

Hodnost tohoto zobrazení $\mathcal{A}$ je rovna nekonečnu, protože $\mathcal{A}(L_1)$ obsahuje určitě všechny polynomy a o lineárním prostoru všech polynomů jsme si řekli v příkladu 2.47, že má nekonečnou bázi.

7.24. Příklad. Zobrazení $\mathcal{A}\colon \mathbf{R}^2 \to \mathbf{R}^3$, $\mathcal{A}(x_1,x_2) = (x_1+2x_2,-x_2,2x_1-3x_2)$ z příkladu 7.11 má defekt roven nule. V příkladu 7.18 jsme totiž ukázali, že $\operatorname{Ker}\mathcal{A} = \{\boldsymbol{o}_1\}$.

Vyšetříme, jak vypadá $\mathcal{A}(L_1)$. Budeme se ptát, pro které hodnoty (y_1,y_2,y_3) existuje dvojice (x_1,x_2) taková, že $\mathcal{A}(x_1,x_2) = (y_1,y_2,y_3)$. Jinými slovy, zjistíme, pro které hodnoty pravých stran má nehomogenní soustava

$$\begin{aligned} x_1 + 2x_2 &= y_1 \\ -\ x_2 &= y_2 \\ 2x_1 - 3x_2 &= y_3 \end{aligned}$$

s neznámými x_1, x_2 nějaké řešení. Eliminujme rozšířenou matici soustavy:

$$\left(\begin{array}{rr|c} 1 & 2 & y_1 \\ 0 & -1 & y_2 \\ 2 & -3 & y_3 \end{array}\right) \sim \left(\begin{array}{rr|c} 1 & 2 & y_1 \\ 0 & 1 & -y_2 \\ 0 & -7 & y_3-2y_1 \end{array}\right) \sim \left(\begin{array}{rr|c} 1 & 2 & y_1 \\ 0 & 1 & -y_2 \\ 0 & 0 & y_3-2y_1-7y_2 \end{array}\right).$$

Podle Frobeniovy věty 5.4 má tato soustava řešení jen tehdy, když $y_3 - 2y_1 - 7y_2 = 0$, tj. $y_3 = 2y_1 + 7y_2$. Z toho nám vychází

$$\mathcal{A}(L_1) = (y_1,y_2,2y_1+7y_2) = y_1\,(1,0,2) + y_2\,(0,1,7), \quad \forall y_1 \in \mathbf{R}, \forall y_2 \in \mathbf{R},$$
$$\mathcal{A}(L_1) = \big\langle(1,0,2),(0,1,7)\big\rangle.$$

Je tedy $\operatorname{hod}\mathcal{A} = \dim \mathcal{A}(L_1) = 2$. Obraz $\mathcal{A}(L_1)$ můžeme spočítat i tak, že spočítáme obrazy báze L_1 a využijeme větu 7.14.

Souřadnice jako lineární zobrazení

7.25. Příklad. Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je uspořádaná báze lineárního prostoru L. Uvažujme zobrazení $\mathcal{A}\colon L \to \mathbf{R}^n$ definované takto

$$\text{nechť} \quad \boldsymbol{x} = (\alpha_1, \alpha_2, \ldots, \alpha_n)_{(B)}, \qquad \text{pak} \quad \mathcal{A}(\boldsymbol{x}) = (\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Ukážeme, že toto zobrazení je lineární a že $\operatorname{def}\mathcal{A} = 0$, $\operatorname{hod}\mathcal{A} = n$.

Nechť $\boldsymbol{x} = (\alpha_1, \alpha_2, \ldots, \alpha_n)_{(B)}$, $\boldsymbol{y} = (\beta_1, \beta_2, \ldots, \beta_n)_{(B)}$. Pro tyto vektory tedy platí

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

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

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

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

Hledejme nyní $\operatorname{Ker}\mathcal{A}$. Z jednoznačnosti souřadnic vzhledem k bázi plyne, že existuje jediný vektor $\boldsymbol{x} = (0, 0, \ldots, 0)_{(B)}$. Protože $\boldsymbol{o} = 0\, \boldsymbol{b}_1 + 0\, \boldsymbol{b}_2 + \cdots + 0\, \boldsymbol{b}_n$, je $\boldsymbol{x} = \boldsymbol{o}$. $\operatorname{Ker}\mathcal{A} = \{\boldsymbol{o}\}$ a $\operatorname{def}\mathcal{A} = 0$.

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

Lineární zobrazení na bázi

7.26. Poznámka. Následující věta ukazuje, že pokud známe hodnoty zobrazení $\mathcal{A}\colon L_1 \to L_2$ jen na bázi lineárního prostoru L_1 a toto zobrazení má být lineární, pak jsou již známy jeho hodnoty na celém prostoru L_1. Jinými slovy, lineární zobrazení je určeno jednoznačně svými hodnotami na bázi L_1.

7.27. Věta. Nechť $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ je báze lineárního prostoru L_1 a nechť jsou dány libovolné vektory $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_n$ z lineárního prostoru L_2. Pak existuje právě jedno lineární zobrazení $\mathcal{A}\colon L_1 \to L_2$, pro které platí

$$\mathcal{A}(\boldsymbol{b}_i) = \boldsymbol{y}_i, \quad \forall i \in \{1, 2, \ldots, n\}. \tag{7.3}$$

Důkaz. (1) Existence. Nechť $\boldsymbol{x} \in L_1$. Protože $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ je báze L_1, existují koeficienty $\alpha_i \in \mathbf{R}$ takové, že $\boldsymbol{x} = \alpha_1 \boldsymbol{b}_1 + \alpha_2 \boldsymbol{b}_2 + \cdots + \alpha_n \boldsymbol{b}_n$. Hodnotu zobrazení $\mathcal{A}$ v bodě $\boldsymbol{x}$ nyní definujeme takto:

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

Zobrazení je lineární a splňuje (7.3). Ukážeme, proč. Čísla $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ jsou souřadnicemi vektoru $\boldsymbol{x}$ vzhledem k uspořádané bázi (B). V příkladu 7.25 jsme ukázali, že

$$\begin{aligned} &\text{je-li} \quad \boldsymbol{x} = (\alpha_1, \alpha_2, \ldots, \alpha_n)_{(B)}, \quad \boldsymbol{y} = (\beta_1, \beta_2, \ldots, \beta_n)_{(B)}, \quad \gamma \in \mathbf{R}, \\ &\text{pak} \quad \boldsymbol{x} + \boldsymbol{y} = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_n + \beta_n)_{(B)}, \quad \gamma\, \boldsymbol{x} = (\gamma\, \alpha_1, \gamma\, \alpha_2, \ldots, \gamma\, \alpha_n)_{(B)}. \end{aligned}$$

Z těchto vlastností okamžitě plyne linearita zobrazení $\mathcal{A}$. Protože souřadnice vektoru $\boldsymbol{b}_i$ vzhledem k bázi (B) jsou všechny nulové s výjimkou i-té souřadnice, která je rovna jedné, platí

$$\mathcal{A}(\boldsymbol{b}_i) = \sum_{\substack{j=0 \\ j \neq i}}^{n} 0 \cdot \boldsymbol{y}_j + 1 \cdot \boldsymbol{y}_i = \boldsymbol{y}_i,$$

což dokazuje požadovanou vlastnost (7.3).

(2) Jednoznačnost. Nechť ještě $\mathcal{B}\colon L_1 \to L_2$ je lineární a splňuje vlastnost (7.3). Pak je lineární i zobrazení $(\mathcal{A}{-}\mathcal{B})\colon L_1 \to L_2$. Platí $(\mathcal{A}{-}\mathcal{B})(\boldsymbol{b}_i) = \boldsymbol{o}$, $\forall i \in \{1, 2, \ldots, n\}$, protože $\mathcal{A}$ i $\mathcal{B}$ splňují vlastnost (7.3). Z linearity zobrazení $\mathcal{A} - \mathcal{B}$ plyne, že

$$\begin{aligned} (\mathcal{A} - \mathcal{B})(\boldsymbol{x}) &= (\mathcal{A} - \mathcal{B})(\alpha_1 \boldsymbol{b}_1 + \alpha_2 \boldsymbol{b}_2 + \cdots + \alpha_n \boldsymbol{b}_n) = \\ &= \alpha_1 (\mathcal{A} - \mathcal{B})(\boldsymbol{b}_1) + \alpha_2 (\mathcal{A} - \mathcal{B})(\boldsymbol{b}_2) + \cdots + \alpha_n (\mathcal{A} - \mathcal{B})(\boldsymbol{b}_n) = \\ &= \alpha_1 \boldsymbol{o} + \alpha_2 \boldsymbol{o} + \cdots + \alpha_n \boldsymbol{o} = \boldsymbol{o}. \end{aligned}$$

Vidíme, že zobrazení $\mathcal{A} - \mathcal{B}$ je nulové na celém definičním oboru, takže $\mathcal{A} = \mathcal{B}$.

7.28. Příklad. Předpokládejme, že $\mathcal{A}\colon \mathbf{R}^3 \to \mathbf{R}^4$ je lineární zobrazení. Najdeme vzorec pro výpočet hodnoty zobrazení $\mathcal{A}(x_1, x_2, x_3)$, je-li známo:

$$\mathcal{A}(1,1,2) = (1,0,1,0), \quad \mathcal{A}(1,2,2) = (2,0,2,0), \quad \mathcal{A}(2,1,5) = (1,2,2,1).$$

Protože jsou vektory $(1,1,2), (1,2,2), (2,1,5)$ lineárně nezávislé a jsou tři, tvoří podle poznámky 2.65 bázi lineárního prostoru $\mathbf{R}^3$. Známe hodnoty hledaného zobrazení na bázi $\mathbf{R}^3$, takže podle věty 7.27 můžeme jednoznačně určit hodnoty $\mathcal{A}$ i v ostatních bodech definičního oboru. Budeme postupovat stejně, jako v důkazu věty 7.27.

Nechť (x_1, x_2, x_3) je libovolný vektor z $\mathbf{R}^3$. Najdeme souřadnice tohoto vektoru vzhledem k uspořádané bázi $\big((1,1,2), (1,2,2), (2,1,5)\big)$:

$$(x_1, x_2, x_3) = \alpha\,(1,1,2) + \beta\,(1,2,2) + \gamma\,(2,1,5).$$

To vede na soustavu tří rovnic o třech neznámých α, β, γ. Eliminujme její rozšířenou matici:

$$\left(\begin{array}{ccc|c} 1 & 1 & 2 & x_1 \\ 1 & 2 & 1 & x_2 \\ 2 & 2 & 5 & x_3 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & 2 & x_1 \\ 0 & 1 & -1 & x_2 - x_1 \\ 0 & 0 & 1 & x_3 - 2x_1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 0 & 8x_1 - x_2 - 3x_3 \\ 0 & 1 & 0 & -3x_1 + x_2 + x_3 \\ 0 & 0 & 1 & x_3 - 2x_1 \end{array}\right).$$

Platí tedy

$$\begin{aligned}
(x_1, x_2, x_3) &= (8x_1 - x_2 - 3x_3)\cdot(1,1,2) + (-3x_1 + x_2 + x_3)\cdot(1,2,2) + (x_3 - 2x_1)\cdot(2,1,5),\\
\mathcal{A}(x_1, x_2, x_3) &= \mathcal{A}\big((8x_1 - x_2 - 3x_3)\cdot(1,1,2) + (-3x_1 + x_2 + x_3)\cdot(1,2,2) + (x_3 - 2x_1)\cdot(2,1,5)\big) =\\
&= (8x_1 - x_2 - 3x_3)\cdot\mathcal{A}(1,1,2) + (-3x_1 + x_2 + x_3)\cdot\mathcal{A}(1,2,2) + (x_3 - 2x_1)\cdot\mathcal{A}(2,1,5) =\\
&= (8x_1 - x_2 - 3x_3)\cdot(1,0,1,0) + (-3x_1 + x_2 + x_3)\cdot(2,0,2,0) + (x_3 - 2x_1)\cdot(1,2,2,1) =\\
&= (x_2,\ -4x_1 + 2x_3,\ -2x_1 + x_2 + x_3,\ -2x_1 + x_3).
\end{aligned}$$

7.29. Věta. Nechť $\mathcal{A}\colon L_1 \to L_2$ je lineární zobrazení. Pak platí: *Zobrazení lineárně nezávislých vektorů*
(1) Jsou-li $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_n$ lineárně závislé vektory v L_1, pak jsou i vektory $\mathcal{A}(\boldsymbol{x}_1), \mathcal{A}(\boldsymbol{x}_2), \dots, \mathcal{A}(\boldsymbol{x}_n)$ lineárně závislé v L_2.
(2) Jsou-li $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_n$ lineárně nezávislé vektory v L_1, pak vektory $\mathcal{A}(\boldsymbol{x}_1), \mathcal{A}(\boldsymbol{x}_2), \dots, \mathcal{A}(\boldsymbol{x}_n)$ v L_2 nemusí být lineárně nezávislé.

Důkaz. (1) Jsou-li $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_n$ lineárně závislé, pak existuje netriviální lineární kombinace, pro kterou je

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

Z věty 7.10 a z linearity zobrazení $\mathcal{A}$ plyne, že

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

Existuje tedy netriviální lineární kombinace vektorů $\mathcal{A}(\boldsymbol{x}_1), \mathcal{A}(\boldsymbol{x}_2), \dots, \mathcal{A}(\boldsymbol{x}_n)$ rovna nulovému vektoru.

(2) Stačí uvést protipříklad. Nechť $\mathcal{A}$ je zobrazení definované v příkladu 7.13, které každé funkci přiřadí její derivaci. Nenulová konstantní funkce je v L_1 lineárně nezávislá, ale zobrazí se na nulovou funkci, která je samozřejmě lineárně závislá.

7.30. Věta. Nechť $\mathcal{A}\colon L_1 \to L_2$ je lineární zobrazení. Následující podmínky jsou ekvivalentní:
(1) $\mathcal{A}$ je prosté.
(2) $\operatorname{def}\mathcal{A} = 0$.
(3) Jsou-li $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_n$ lineárně nezávislé, jsou lineárně nezávislé i vektory $\mathcal{A}(\boldsymbol{x}_1), \mathcal{A}(\boldsymbol{x}_2), \dots, \mathcal{A}(\boldsymbol{x}_n)$.

Důkaz. Ekvivalenci těchto podmínek ověříme tak, že dokážeme (1) $\Rightarrow$ (2), (2) $\Rightarrow$ (3) a (3) $\Rightarrow$ (1).

(1) $\Rightarrow$ (2): Je-li $\mathcal{A}$ prosté, pak podle definice 7.5 pouze jeden prvek z L_1 se může zobrazit na nulový prvek z L_2. Protože $\mathcal{A}$ je lineární, musí tím prvkem být nulový prvek. Platí tedy $\operatorname{Ker}\mathcal{A} = \{\boldsymbol{o}\}$, $\operatorname{def}\mathcal{A} = \dim\operatorname{Ker}\mathcal{A} = 0$.

(2) $\Rightarrow$ (3): Ověříme lineární nezávislost vektorů $\mathcal{A}(\boldsymbol{x}_1), \mathcal{A}(\boldsymbol{x}_2), \dots, \mathcal{A}(\boldsymbol{x}_n)$. Položíme proto

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

a vyzkoumáme, co z toho plyne pro koeficienty $\alpha_1, \alpha_2, \ldots, \alpha_n$. Z linearity zobrazení $\mathcal{A}$ plyne

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

Podle definice jádra zobrazení 7.16 je tedy $(\alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_n \boldsymbol{x}_n) \in \operatorname{Ker} \mathcal{A}$. Podle předpokladu (2) jádro obsahuje pouze nulový vektor, tj.

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

Protože vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou lineárně nezávislé, musí $\alpha_i = 0, \forall i \in \{1, 2, \ldots, n\}$. Tím jsme dokázali, že i vektory $\mathcal{A}(\boldsymbol{x}_1), \mathcal{A}(\boldsymbol{x}_2), \ldots, \mathcal{A}(\boldsymbol{x}_n)$ jsou lineárně nezávislé.

(3) $\Rightarrow$ (1): Nechť $\boldsymbol{x} \in L_1$, $\boldsymbol{y} \in L_1$, $\boldsymbol{x} \neq \boldsymbol{y}$. Dokážeme, že pak $\mathcal{A}(\boldsymbol{x}) \neq \mathcal{A}(\boldsymbol{y})$. Vektor $\boldsymbol{x} - \boldsymbol{y} \neq \boldsymbol{o}$ je sám o sobě lineárně nezávislý. Podle (3) musí být lineárně nezávislý i vektor $\mathcal{A}(\boldsymbol{x} - \boldsymbol{y})$. Je tedy $\mathcal{A}(\boldsymbol{x} - \boldsymbol{y}) \neq \boldsymbol{o}$ a z linearity zobrazení $\mathcal{A}$ plyne $\mathcal{A}(\boldsymbol{x}) \neq \mathcal{A}(\boldsymbol{y})$.

Složené zobrazení

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

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

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

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

Inverzní zobrazení

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

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

Důkaz. Pro každý prvek $\boldsymbol{y} \in \mathcal{A}(L_1)$ existuje právě jeden prvek $\boldsymbol{x} \in L_1$ takový, že $\mathcal{A}(\boldsymbol{x}) = \boldsymbol{y}$. To plyne přímo z definice 7.5 prostého zobrazení. Definujeme $\mathcal{A}^{-1}(\boldsymbol{y}) = \boldsymbol{x}$. Vidíme, že $\mathcal{A}^{-1} \circ \mathcal{A}$ je identita.

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

Důkaz. Identita je zcela zřejmě lineární. Ověříme linearitu zobrazení $\mathcal{A}^{-1}$. Počítejme $\mathcal{A}^{-1}(\boldsymbol{x} + \boldsymbol{y})$ pro $\boldsymbol{x} \in \mathcal{A}(L_1)$, $\boldsymbol{y} \in \mathcal{A}(L_1)$. Podle věty 7.20 je $\mathcal{A}(L_1)$ lineární podprostor, takže $\boldsymbol{x} + \boldsymbol{y} \in \mathcal{A}(L_1)$. Protože $\mathcal{A}$ je prosté, existuje právě jeden vektor $\boldsymbol{a} \in L_1$ a právě jeden vektor $\boldsymbol{b} \in L_1$ tak, že $\mathcal{A}(\boldsymbol{a}) = \boldsymbol{x}$, $\mathcal{A}(\boldsymbol{b}) = \boldsymbol{y}$. Platí tedy $\mathcal{A}^{-1}(\boldsymbol{x}) = \boldsymbol{a}$, $\mathcal{A}^{-1}(\boldsymbol{y}) = \boldsymbol{b}$. Protože $\mathcal{A}$ je lineární, je $\mathcal{A}(\boldsymbol{a} + \boldsymbol{b}) = \boldsymbol{x} + \boldsymbol{y}$, neboli

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

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

7.36. Věta. Nechť $\mathcal{A}\colon L_1 \to L_2$ je lineární, prosté a „na“ L_2. Pak je inverzní zobrazení $\mathcal{A}^{-1}\colon L_2 \to L_1$ rovněž lineární, prosté a „na“ L_1.

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

Že je $\mathcal{A}^{-1}$ lineární plyne z věty 7.35.

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

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

7.37. Definice. Zobrazení $\mathcal{A}: L_1 \to L_2$ nazýváme *izomorfismus*, pokud je lineární, prosté a „na“ L_2. *Izomorfismus*

Lineární prostor L_1 nazýváme *izomorfní s* L_2, pokud existuje izomorfismus $\mathcal{A}: L_1 \to L_2$. Protože k prostému lineárnímu zobrazení, které je „na“ L_2, existuje inverzní zobrazení $\mathcal{A}^{-1}: L_2 \to L_1$, které je podle věty 7.36 rovněž izomorfismem, platí: je-li L_1 izomorfní s L_2, je též L_2 izomorfní s L_1. Často proto říkáme, že L_1 a L_2 jsou (vzájemně) izomorfní.

7.38. Poznámka. Izomorfismus $\mathcal{A}: L_1 \to L_2$ převádí podle věty 7.30 lineárně nezávislé vektory v L_1 na lineárně nezávislé vektory v L_2. Protože je lineární, pak přenáší i další pojmy „linearity“ z L_1 do L_2: lineární závislost (věta 7.29), lineární obaly (věta 7.14), podprostory (poznámka 7.15) a báze. Jsou-li L_1 a L_2 izomorfní, je tedy jedno, zda při vyšetřování „lineárních záležitostí“ se pohybujeme v L_1 nebo v L_2. Veškeré struktury přeneseme prostřednictvím izomorfismu do takového lineárního prostoru, se kterým se nám lépe pracuje. Z tohoto pohledu je pro nás důležitá následující věta.

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

Důkaz. Protože $\dim L = n$, existuje konečná báze $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ lineárního prostoru L. Uspořádejme tuto bázi a označme ji (B). Příklad 7.25 ukazuje, že zobrazení $\mathcal{A}: L \to \mathbf{R}^n$, které každému prvku $\boldsymbol{x} \in L$ přiřadí jeho souřadnice vzhledem k bázi (B), je lineární, je „na“ $\mathbf{R}^n$ a platí pro ně $\operatorname{def} \mathcal{A} = 0$. Podle věty 7.30 je toto zobrazení prosté, takže podle definice 7.37 jde o izomorfismus.

7.40. Poznámka. Se všemi lineárními prostory konečné dimenze můžeme tedy pracovat stejně jako s $\mathbf{R}^n$. Stačí v lineárním prostoru najít nějakou bázi a dále už jen pracovat se souřadnicemi vzhledem k této bázi. Setkali jsme se například s lineárním prostorem všech polynomů nejvýše n-tého stupně, který je izomorfní s $\mathbf{R}^{n+1}$, s lineárním prostorem matic typu (m, n), který je izomorfní s $\mathbf{R}^{m \cdot n}$ a s lineárním prostorem orientovaných úseček, který je izomorfní s $\mathbf{R}^3$.

7.41. Věta. Nechť $\mathcal{A}: L_1 \to L_2$ a $\mathcal{B}: L_2 \to L_3$ jsou izomorfismy. Pak je izomorfismem i složené zobrazení $(\mathcal{B} \circ \mathcal{A}): L_1 \to L_3$.

Důkaz. Že je $\mathcal{B} \circ \mathcal{A}$ lineární, dokazuje věta 7.32. Ukážeme, že je $\mathcal{B} \circ \mathcal{A}$ prosté. Nechť $\boldsymbol{x} \in L_1$, $\boldsymbol{y} \in L_1$, $\boldsymbol{x} \neq \boldsymbol{y}$. Pak platí $\mathcal{A}(\boldsymbol{x}) \neq \mathcal{A}(\boldsymbol{y})$, protože $\mathcal{A}$ je prosté. Také platí $\mathcal{B}\big(\mathcal{A}(\boldsymbol{x})\big) \neq \mathcal{B}\big(\mathcal{A}(\boldsymbol{y})\big)$, protože je $\mathcal{B}$ prosté. Tím jsme dokázali, že $(\mathcal{B} \circ \mathcal{A})(\boldsymbol{x}) \neq (\mathcal{B} \circ \mathcal{A})(\boldsymbol{y})$.

Ukážeme ještě, že je $\mathcal{B} \circ \mathcal{A}$ „na“ L_3. Protože je $\mathcal{A}(L_1) = L_2$ a $\mathcal{B}(L_2) = L_3$, je též

$$(\mathcal{B} \circ \mathcal{A})(L_1) = \mathcal{B}\big(\mathcal{A}(L_1)\big) = \mathcal{B}(L_2) = L_3.$$

7.42. Věta. Dva lineární prostory konečné dimenze jsou izomorfní právě tehdy, když se rovnají jejich dimenze.

Důkaz. Nechť $\dim L_1 = \dim L_2 = n$. Oba lineární prostory jsou izomorfní s $\mathbf{R}^n$ podle věty 7.39. Nechť $\mathcal{A}: L_1 \to \mathbf{R}^n$ a $\mathcal{B}: L_2 \to \mathbf{R}^n$ jsou izomorfismy. Pak podle věty 7.36 je též $\mathcal{B}^{-1}: \mathbf{R}^n \to L_2$ izomorfismem a podle věty 7.41 je $(\mathcal{B}^{-1} \circ \mathcal{A}): L_1 \to L_2$ izomorfismus.

Nechť naopak $\dim L_1 \neq \dim L_2$. Protože izomorfismus převádí podle věty 7.30 lineárně nezávislé vektory na lineárně nezávislé vektory, převádí bázi v L_1 na bázi v L_2. Takové báze pak musejí mít stejný počet prvků, což je spor s předpokladem $\dim L_1 \neq \dim L_2$, takže izomorfismus $\mathcal{A}: L_1 \to L_2$ neexistuje.

7.43. Definice. Nechť L_1 a L_2 jsou lineární prostory konečné dimenze, $\mathcal{A}: L_1 \to L_2$ je lineární. Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je uspořádaná báze L_1 a $(C) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m)$ je uspořádaná báze L_2. Matici $\mathbf{A}$ typu (m, n), která splňuje maticovou rovnost *Matice lineárního zobrazení*

$$\big(\mathcal{A}(\boldsymbol{b}_1), \mathcal{A}(\boldsymbol{b}_2), \ldots, \mathcal{A}(\boldsymbol{b}_n)\big) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m) \cdot \mathbf{A}, \tag{7.4}$$

nazýváme *maticí zobrazení $\mathcal{A}$ vzhledem k uspořádaným bázím (B) a (C)*. Na definiční rovnost (7.4) se díváme jako na součin jednořádkové matice vektorů $(\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m)$ s maticí $\mathbf{A}$ reálných čísel typu (m, n), který se má rovnat jednořádkové matici vektorů $\big(\mathcal{A}(\boldsymbol{b}_1), \mathcal{A}(\boldsymbol{b}_2), \ldots, \mathcal{A}(\boldsymbol{b}_n)\big)$.

7.44. Věta. Nechť platí předpoklady z definice 7.43. Pak matice $\mathbf{A}$ zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C) existuje a je určena jednoznačně.

Důkaz. Povšimneme si, že i-tý sloupec matice $\mathbf{A}$ obsahuje souřadnice vektoru $\mathcal{A}(\boldsymbol{b}_i)$ vzhledem k bázi (C). To plyne přímo z definiční rovnosti (7.4) a z definice součinu matic. Máme tedy metodu, jak sestavit matici zobrazení.

Vzhledem k tomu, že jsou souřadnice vektoru vzhledem k bázi (C) určeny jednoznačně, je i matice $\mathbf{A}$ zobrazení $\mathcal{A}$ určena tímto zobrazením a bázemi (B) a (C) jednoznačně.

7.45. Věta. Nechť L_1, L_2 jsou lineární prostory konečné dimenze, $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je uspořádaná báze L_1 a $(C) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m)$ je uspořádaná báze L_2. Pak ke každé matici $\mathbf{A}$ typu (m, n) existuje právě jedno lineární zobrazení $\mathcal{A}\colon L_1 \to L_2$ takové, že $\mathbf{A}$ je maticí zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C).

Důkaz. Rovnost (7.4) udává hodnoty zobrazení $\mathcal{A}$ na prvcích báze B. Z věty 7.27 víme, že známe-li hodnoty lineárního zobrazení na bázi, je toto lineární zobrazení určeno jednoznačně na celém definičním oboru.

7.46. Poznámka. Předchozí dvě věty ukazují, že pokud pevně zvolíme báze (B) v L_1 a (C) v L_2, pak je lineární zobrazení určeno svou maticí jednoznačně a obráceně, lineární zobrazení jednoznačně určuje svou matici. Místo lineárních zobrazení na lineárních prostorech konečné dimenze se tak můžeme zabývat jen maticemi těchto zobrazení bez ztráty informace.

7.47. Poznámka. Transponujeme-li definiční rovnost (7.4), dostáváme maticovou rovnost

$$\begin{pmatrix} \mathcal{A}(\boldsymbol{b}_1) \\ \vdots \\ \mathcal{A}(\boldsymbol{b}_n) \end{pmatrix} = \mathbf{A}^T \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix},$$

se kterou se můžeme setkat v některých učebnicích jako s definiční rovností pro matici lineárního zobrazení $\mathcal{A}$. Všimněme si, že se zde pracuje s maticí transponovanou k matici lineárního zobrazení.

7.48. Věta. Nechť (B) je báze v L_1, (C) je báze v L_2, $\mathcal{A}\colon L_1 \to L_2$ je lineární a $\mathbf{A}$ je maticí zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C). Pak $\operatorname{hod}\mathbf{A} = \operatorname{hod}\mathcal{A}$. *Hodnost matice zobrazení*

Důkaz. Označíme-li symboly $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ jednotlivé sloupce matice $\mathbf{A}$, pak platí:

$$\begin{aligned} \operatorname{hod}\mathcal{A} &= \dim \mathcal{A}(L_1) = \dim \mathcal{A}(\langle B\rangle) = \dim\langle \mathcal{A}(B)\rangle = \dim \langle \mathcal{A}(\boldsymbol{b}_1), \mathcal{A}(\boldsymbol{b}_2), \ldots, \mathcal{A}(\boldsymbol{b}_n)\rangle = \\ &= \dim\big\langle (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m)\cdot \mathbf{A}_1, (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m)\cdot \mathbf{A}_2, \ldots, (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m)\cdot \mathbf{A}_n\big\rangle = \\ &= \dim \langle \mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n\rangle = \operatorname{hod}\mathbf{A}. \end{aligned}$$

V uvedené řadě rovností jsme nejprve použili definici hodnosti zobrazení 7.21, dále vlastnosti báze, dále větu 7.14, pak jsme rozepsali množinu $\mathcal{A}(B)$ výčtem prvků, dále jsme využili rovnost (7.4) a konečně jsme využili toho, že maximální počet lineárně nezávislých vektorů z množiny $\{\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n\}$ (věta 3.18) je roven maximálnímu počtu lineárně nezávislých vektorů ze „skoro stejné“ množiny, jen každý vektor je násoben stejným řádkem lineárně nezávislých vektorů $(\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m)$. Úplně poslední rovnost je v souladu s definicí hodnosti matice 3.15 při použití věty 3.31.

7.49. Věta. Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je báze v L_1, $(C) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m)$ je báze v L_2, $\mathcal{A}\colon L_1 \to L_2$ je lineární a $\mathbf{A}$ je maticí zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C). Pak pro každý vektor $\boldsymbol{x} \in L_1$, $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)_{(B)}$, platí pro souřadnice vektoru $\mathcal{A}(\boldsymbol{x}) = (y_1, y_2, \ldots, y_m)_{(C)}$ následující rovnost: *Zobrazení souřadnic*

$$\mathbf{A}\cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}. \tag{7.5}$$

Důkaz. Označme $\mathbf{A} = (a_{i,j})$, $i \in \{1,2,\ldots,m\}$, $j \in \{1,2,\ldots,n\}$. Protože $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)_{(B)}$, je podle definice 6.10 $\boldsymbol{x} = x_1\,\boldsymbol{b}_1 + x_2\,\boldsymbol{b}_2 + \cdots + x_n\,\boldsymbol{b}_n$. Pro vektor $\mathcal{A}(\boldsymbol{x})$ platí:

$$\begin{aligned}
\mathcal{A}(\boldsymbol{x}) &= \mathcal{A}(x_1\,\boldsymbol{b}_1 + x_2\,\boldsymbol{b}_2 + \cdots + x_n\,\boldsymbol{b}_n) = x_1\mathcal{A}(\boldsymbol{b}_1) + x_2\mathcal{A}(\boldsymbol{b}_2) + \cdots + x_n\mathcal{A}(\boldsymbol{b}_n) = \\
&= x_1\,(\boldsymbol{c}_1\,a_{1,1} + \boldsymbol{c}_2\,a_{2,1} + \cdots + \boldsymbol{c}_m\,a_{m,1}) + x_2\,(\boldsymbol{c}_1\,a_{1,2} + \boldsymbol{c}_2\,a_{2,2} + \cdots + \boldsymbol{c}_m\,a_{m,2}) + \cdots + \\
&\qquad + \cdots + x_n\,(\boldsymbol{c}_1\,a_{1,n} + \boldsymbol{c}_2\,a_{2,n} + \cdots + \boldsymbol{c}_m\,a_{m,n}) = \\
&= \boldsymbol{c}_1\,(a_{1,1}\,x_1 + a_{1,2}\,x_2 + \cdots + a_{1,n}\,x_n) + \boldsymbol{c}_2\,(a_{2,1}\,x_2 + a_{2,2}\,x_2 + \cdots + a_{2,n}\,x_n) + \cdots + \\
&\qquad + \cdots + \boldsymbol{c}_m\,(a_{m,1}\,x_2 + a_{m,2}\,x_2 + \cdots + a_{m,n}\,x_n) = \\
&= y_1\,\boldsymbol{c}_1 + y_2\,\boldsymbol{c}_2 + \cdots + y_m\,\boldsymbol{c}_m.
\end{aligned}$$

Z definice 6.10 vidíme, že čísla y_j jsou souřadnicemi vektoru $\mathcal{A}(\boldsymbol{x})$ vzhledem k bázi (C). Z poslední rovnosti našeho výpočtu plyne, že $y_j = a_{j,1}\,x_2 + a_{j,2}\,x_2 + \cdots + a_{j,n}\,x_n$, $\forall j \in \{1,2,\ldots,m\}$, což ale podle definice maticového násobení 3.34 není nic jiného, než dokazovaný vzorec (7.5).

7.50. Poznámka. Právě dokázaná věta dává jednoduchý návod, jak počítat souřadnice hodnot zobrazení $\mathcal{A}$, známe-li matici tohoto zobrazení.

7.51. Příklad. Vraťme se k příkladu 7.28. Je dáno zobrazení $\mathcal{A}\colon \mathbf{R}^3 \to \mathbf{R}^4$. V příkladu jsme vypočítali, že

$$\mathcal{A}(x_1, x_2, x_3) = (x_2,\ -4x_1 + 2x_3,\ -2x_1 + x_2 + x_3,\ -2x_1 + x_3).$$

Najdeme matici $\mathbf{A}$ tohoto zobrazení vzhledem ke standardním bázím.

Protože složky (x_1, x_2, x_3) i složky hodnot zobrazení $\mathcal{A}$ jsou podle věty 6.29 současně souřadnicemi vzhledem ke standardním bázím, můžeme podle věty 7.49 psát:

$$\mathbf{A} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_2 \\ -4x_1 + 2x_3 \\ -2x_1 + x_2 + x_3 \\ -2x_1 + x_3 \end{pmatrix}.$$

Z této maticové rovnosti můžeme okamžitě zapsat prvky matice $\mathbf{A}$. V každém řádku této matice jsou koeficienty lineární kombinace čísel x_1, x_2, x_3, které vedou na výsledek v odpovídajícím řádku na pravé straně. Je tedy

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 \\ -4 & 0 & 2 \\ -2 & 1 & 1 \\ -2 & 0 & 1 \end{pmatrix}.$$

7.52. Příklad. Ještě jednou se vrátíme k příkladu 7.28. Označme

$$(B) = \big((1,1,2), (1,2,2), (2,5,1)\big).$$

V příkladu jsme ověřili, že se jedná o bázi v $\mathbf{R}^3$. Najdeme matici $\mathbf{A}'$ zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (S), kde symbolem (S) značíme standardní uspořádanou bázi v $\mathbf{R}^4$.

Zopakujme zadání příkladu:

$$\mathcal{A}(1,1,2) = (1,0,1,0), \quad \mathcal{A}(1,2,2) = (2,0,2,0), \quad \mathcal{A}(2,1,5) = (1,2,2,1).$$

Podle důkazu věty 7.44 obsahuje i-tý sloupec matice $\mathbf{A}'$ souřadnice vektoru $\mathcal{A}(\boldsymbol{b}_i)$ vzhledem k bázi (S). Protože se jedná o standardní bázi, jsou tyto souřadnice přímo složkami vektorů $\mathcal{A}(\boldsymbol{b}_i)$. Můžeme tedy přímo zapsat matici $\mathbf{A}'$ zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (S):

$$\mathbf{A}' = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 2 \\ 1 & 2 & 2 \\ 0 & 0 & 1 \end{pmatrix}. \tag{7.6}$$

7.53. Věta. Nechť L_1, L_2 jsou lineární prostory konečné dimenze, $\mathcal{A}\colon L_1 \to L_2$ je lineární. Pak *Defekt + hodnost zobrazení*

$$\operatorname{def}\mathcal{A} + \operatorname{hod}\mathcal{A} = \dim L_1.$$

Důkaz. Zvolme nějakou bázi (B) v L_1 a bázi (C) v L_2. Nechť $\mathbf{A}$ je matice zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C). Podle věty 7.49 je

$$\operatorname{Ker}\mathcal{A} = \bigl\{\boldsymbol{x} \in L_1;\ \mathcal{A}(\boldsymbol{x}) = \boldsymbol{o}\bigr\} = \left\{\boldsymbol{x} \in L_1;\ \boldsymbol{x} = (x_1, x_2, \ldots, x_n)_{(B)} \quad \text{a} \quad \mathbf{A} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}\right\}.$$

Protože z příkladu 7.25 víme, že zobrazení, které vektoru $\boldsymbol{x}$ přiřadí jeho souřadnice, je izomorfismem, platí

$$\operatorname{def}\mathcal{A} = \dim\operatorname{Ker}\mathcal{A} = \dim\bigl\{\boldsymbol{x} \in L_1;\ \mathcal{A}(\boldsymbol{x}) = \boldsymbol{o}\bigr\} = \dim\bigl\{\boldsymbol{a} \in \mathbf{R}^n;\ \mathbf{A} \cdot \boldsymbol{a}^T = \boldsymbol{o}^T\bigr\}.$$

Vidíme, že $\operatorname{def}\mathcal{A}$ je roven dimenzi prostoru řešení homogenní soustavy s maticí soustavy $\mathbf{A}$. Podle věty 5.13 je tato dimenze rovna $k = n - \operatorname{hod}\mathbf{A}$, kde n je počet neznámých soustavy. Počet neznámých je v tomto případě roven počtu prvků báze B, takže je roven $\dim L_1$.

Dostáváme výsledek $\operatorname{def}\mathcal{A} = \dim L_1 - \operatorname{hod}\mathbf{A} = \dim L_1 - \operatorname{hod}\mathcal{A}$. V poslední rovnosti jsme použili větu 7.48.

7.54. Příklad. Je dáno lineární zobrazení $\mathcal{A}\colon \mathbf{R}^4 \to \mathbf{R}^3$ předpisem

$$\mathcal{A}(x_1, x_2, x_3, x_4) = (x_1 + 2x_2 + 2x_3 + 3x_4,\ x_1 + 2x_2 + 4x_3 + 7x_4,\ 2x_1 + 4x_2 + 3x_3 + 4x_4).$$

Najdeme matici zobrazení $\mathcal{A}$ vzhledem ke standardním bázím. Dále najdeme $\operatorname{Ker}\mathcal{A}$, $\operatorname{def}\mathcal{A}$ a $\operatorname{hod}\mathcal{A}$.

Podobně jako v příkladu 7.51 sestavíme matici lineárního zobrazení vzhledem ke standardním bázím tak, že zapíšeme koeficienty lineárních kombinací čísel x_1, x_2, x_3, x_4 do řádků matice:

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 2 & 3 \\ 1 & 2 & 4 & 7 \\ 2 & 4 & 3 & 4 \end{pmatrix}.$$

Podle důkazu věty 7.53 je $\operatorname{Ker}\mathcal{A}$ roven množině všech řešení homogenní soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$. Eliminujeme tedy matici soustavy a najdeme všechna řešení

$$\begin{pmatrix} 1 & 2 & 2 & 3 \\ 1 & 2 & 4 & 7 \\ 2 & 4 & 3 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 2 & 3 \\ 0 & 0 & 2 & 4 \\ 0 & 0 & -1 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 2 & 3 \\ 0 & 0 & 1 & 2 \end{pmatrix}.$$

Při $x_4 = t$, $x_2 = u$ je $x_3 = -2t$, $x_1 = -2u - 2(-2t) - 3t = t - 2u$. Jinak napsáno je:

$$(x_1, x_2, x_3, x_4) = (t - 2u, u, -2t, t) = t\,(1, 0, -2, 1) + u\,(-2, 1, 0, 0),$$
$$\operatorname{Ker}\mathcal{A} = \bigl\langle (1, 0, -2, 1), (-2, 1, 0, 0) \bigr\rangle.$$

Dále je $\operatorname{def}\mathcal{A} = \dim\operatorname{Ker}\mathcal{A} = 2$, $\operatorname{hod}\mathcal{A} = \operatorname{hod}\mathbf{A} = 2$. Podle věty 7.53 je skutečně $2 + 2 = \dim\mathbf{R}^4$.

7.55. Věta. Nechť L_1, L_2, L_3 jsou lineární prostory konečné dimenze, $\mathcal{A}\colon L_1 \to L_2$, $\mathcal{B}\colon L_2 \to L_3$ jsou lineární zobrazení. Nechť dále (B) je uspořádaná báze L_1, (C) je uspořádaná báze L_2 a (D) je uspořádaná báze L_3. Předpokládejme ještě, že $\mathbf{A}$ je matice zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C) a konečně $\mathbf{B}$ 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). *Matice složeného zobrazení*

Důkaz. Při označení $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$, $(C) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m)$, $(D) = (\boldsymbol{d}_1, \boldsymbol{d}_2, \ldots, \boldsymbol{d}_k)$ podle definice 7.43 platí:

$$\bigl(\mathcal{A}(\boldsymbol{b}_1), \mathcal{A}(\boldsymbol{b}_2), \ldots, \mathcal{A}(\boldsymbol{b}_n)\bigr) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m) \cdot \mathbf{A}, \qquad \bigl(\mathcal{B}(\boldsymbol{c}_1), \mathcal{B}(\boldsymbol{c}_2), \ldots, \mathcal{B}(\boldsymbol{c}_m)\bigr) = (\boldsymbol{d}_1, \boldsymbol{d}_2, \ldots, \boldsymbol{d}_k) \cdot \mathbf{B}.$$

Protože $\mathcal{B}$ je lineární, platí

$$\Bigl(\mathcal{B}\bigl(\mathcal{A}(\boldsymbol{b}_1)\bigr), \mathcal{B}\bigl(\mathcal{A}(\boldsymbol{b}_2)\bigr), \ldots, \mathcal{B}\bigl(\mathcal{A}(\boldsymbol{b}_n)\bigr)\Bigr) = \bigl(\mathcal{B}(\boldsymbol{c}_1), \mathcal{B}(\boldsymbol{c}_2), \ldots, \mathcal{B}(\boldsymbol{c}_m)\bigr) \cdot \mathbf{A} = (\boldsymbol{d}_1, \boldsymbol{d}_2, \ldots, \boldsymbol{d}_k) \cdot \mathbf{B} \cdot \mathbf{A}.$$

Podle definice 7.31 je $\mathcal{B}\bigl(\mathcal{A}(\boldsymbol{x})\bigr) = (\mathcal{B} \circ \mathcal{A})(\boldsymbol{x})$, takže $\mathbf{B} \cdot \mathbf{A}$ je maticí zobrazení $\mathcal{B} \circ \mathcal{A}$ vzhledem k bázím (B) a (D).

7.56. Věta. Nechť (B) a (C) jsou dvě báze lineárního prostoru L. Pak matice identického zobrazení $\mathcal{I}\colon L \to L$ vzhledem k bázím (B) a (C) je rovna matici přechodu $\mathbf{A}_{(C,B)}$ od báze (C) k bázi (B). *Matice identity*

Důkaz. Nechť $\mathbf{A}$ je matice identity vzhledem k bázím (B) a (C). Podle (7.4) je

$$\big(\mathcal{I}(\boldsymbol{b}_1), \mathcal{I}(\boldsymbol{b}_2), \ldots, \mathcal{I}(\boldsymbol{b}_n)\big) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n) \cdot \mathbf{A}.$$

Tato podmínka je ekvivalentní s definicí 6.18 matice přechodu od báze (C) k bázi (B).

7.57. Příklad. Zkusíme se naposledy vrátit k příkladu 7.28. V původním zadání byly dány hodnoty zobrazení $\mathcal{A}$ pouze na bázi a našim úkolem bylo zjistit, jak vypadá $\mathcal{A}$ na celém definičním oboru. Pokusíme se příklad vyřešit ještě jednou, tentokrát s použitím matic zobrazení vzhledem k různým bázím.

Cílem je najít matici zobrazení vzhledem ke standardním bázím. Uveďme báze, se kterými budeme pracovat:

$$(B) = \big((1,1,2),(1,2,2),(2,1,5)\big), \qquad (S_0) = \big((1,0,0),(0,1,0),(0,0,1)\big),$$
$$(S) = \big((1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\big).$$

Známe matici $\mathbf{A}'$ zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (S), viz (7.6) v příkladu 7.52. Nechť $\mathbf{A}_{(B,S_0)}$ je matice přechodu od báze (B) k bázi (S_0). Podle věty 7.56 je to zároveň matice identity vzhledem k bázím (S_0) a (B). Podle věty 7.55 se matice $\mathbf{A}$ složeného zobrazení $\mathcal{A} \circ \mathcal{I}$ vzhledem k bázím (S_0) a (S) počítá takto:

$$\mathbf{A} = \mathbf{A}' \cdot \mathbf{A}_{(B,S_0)}.$$

Matice $\mathbf{A}$ je hledanou maticí zobrazení $\mathcal{A}$ vzhledem ke standardním bázím, protože $\mathcal{A} \circ \mathcal{I} = \mathcal{A}$. Stačí tedy spočítat matici přechodu $\mathbf{A}_{(B,S_0)}$ a provést uvedené maticové násobení.

Matice přechodu $\mathbf{A}_{(S_0,B)}$ od báze (S_0) k bázi (B) obsahuje ve sloupcích přímo složky vektorů báze (B) (viz například větu 6.30). My bohužel potřebujeme najít matici přechodu od (B) k (S_0). Budeme počítat inverzní matici, protože podle věty 6.21 je $\mathbf{A}_{(B,S_0)} = \mathbf{A}^{-1}_{(S_0,B)}$. Níže uvádíme závěrečné výpočty:

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 2 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 & 1 & 0 \\ 2 & 2 & 5 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 1 & 2 & 1 & 0 & 0 \\ 0 & 2 & -1 & -1 & 1 & 0 \\ 0 & 0 & 1 & -2 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 8 & -1 & -3 \\ 0 & 1 & 0 & -3 & 1 & 1 \\ 0 & 0 & 1 & -2 & 0 & 1 \end{array}\right),$$

$$\mathbf{A} = \mathbf{A}' \cdot \mathbf{A}_{(B,S_0)} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 2 \\ 1 & 2 & 2 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 8 & -1 & -3 \\ -3 & 1 & 1 \\ -2 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ -4 & 0 & 2 \\ -2 & 1 & 1 \\ -2 & 0 & 1 \end{pmatrix}.$$

7.58. Poznámka. Při použití věty 7.56 vychází věta 6.23 jako důsledek věty 7.49: je-li $\mathbf{A}_{(B,C)}$ maticí přechodu od báze (B) k bázi (C), pak podle věty 6.21 je $\mathbf{A}^{-1}_{(B,C)}$ maticí přechodu od báze (C) k bázi (B). Podle věty 7.56 je $\mathbf{A}^{-1}_{(B,C)}$ rovněž maticí identity vzhledem k bázím (B) a (C). Nyní použijeme větu 7.49. Nechť $\boldsymbol{x} \in L$, $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)_{(B)}$, $\mathcal{I}(\boldsymbol{x}) = \boldsymbol{x} = (y_1, y_2, \ldots, y_n)_{(C)}$, pak platí

$$\mathbf{A}^{-1}_{(B,C)} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Po vynásobení maticí $\mathbf{A}_{(B,C)}$ zleva dostáváme tvrzení věty 6.23.

$$\mathbf{A}_{(B,C)} \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

7.59. Věta. Nechť $\mathcal{A}: L_1 \to L_2$ je lineární zobrazení a nechť (B_1), (C_1) jsou báze lineárního prostoru L_1 a (B_2), (C_2) jsou báze lineárního prostoru L_2. Označme symbolem $\mathbf{A}_{(B_1,C_1)}$ matici přechodu od báze (B_1) k (C_1) a $\mathbf{A}_{(C_2,B_2)}$ matici přechodu od báze (C_2) k (B_2). Je-li $\mathbf{A}$ matice zobrazení $\mathcal{A}$ vzhledem k bázím (B_1), (B_2), pak $\mathbf{A}_{(C_2,B_2)} \cdot \mathbf{A} \cdot \mathbf{A}_{(B_1,C_1)}$ je matice téhož lineárního zobrazení vzhledem k bázím (C_1), (C_2).

Důkaz. Matice $\mathbf{A}_{(B_1,C_1)}$ je podle věty 7.56 maticí identického zobrazení $\mathcal{I}_1 : L_1 \to L_1$ vzhledem k bázím (C_1) a (B_1). Stejně tak matice $\mathbf{A}_{(C_2,B_2)}$ je maticí identity $\mathcal{I}_2 : L_2 \to L_2$ vzhledem k bázím (B_2) a (C_2). Dále si stačí uvědomit, že $\mathcal{A} = \mathcal{I}_2 \circ \mathcal{A} \circ \mathcal{I}_1$ a použít větu 7.55.

7.60. Definice. Nechť $\mathcal{A}: L \to L$ je lineární zobrazení (lineární prostor vzorů i obrazů je stejný a má konečnou dimenzi). Místo, abychom mluvili o matici lineárního zobrazení vzhledem ke stejným bázím (B) a (B) (to působí, jako bychom koktali), stručně se zmiňujeme o *matici zobrazení $\mathcal{A}$ vzhledem k bázi* (B).

Zobrazení do stejného prostoru

7.61. Věta. Nechť $\mathcal{A}: L \to L$ je lineární zobrazení, (B), (C) jsou dvě báze lineárního prostoru L a $\mathbf{A}_{(B,C)}$ je matice přechodu od báze (B) k bázi (C). Je-li $\mathbf{A}$ matice zobrazení $\mathcal{A}$ vzhledem k bázi (B), pak $\mathbf{A}^{-1}_{(B,C)} \cdot \mathbf{A} \cdot \mathbf{A}_{(B,C)}$ je maticí téhož lineárního zobrazení vzhledem k bázi (C).

Důkaz. $\mathbf{A}^{-1}_{(B,C)}$ je podle věty 6.21 maticí přechodu od (C) k (B). Zbytek plyne z věty 7.59.

7.62. Poznámka. Protože možné matice přechodu od báze k bázi jsou právě všechny regulární matice, můžeme na základě předchozí věty říci, že dvě matice $\mathbf{A}$, $\mathbf{B}$ jsou maticemi stejného lineárního zobrazení $\mathcal{A}: L \to L$ právě tehdy, když existuje regulární matice $\mathbf{P}$ taková, že $\mathbf{B} = \mathbf{P}^{-1} \cdot \mathbf{A} \cdot \mathbf{P}$. Tyto matice se tedy z pohledu lineárního zobrazení příliš neliší, což vystihuje následující definice:

7.63. Definice. Matice $\mathbf{A}$ je *podobná* matici $\mathbf{B}$, pokud existuje regulární matice $\mathbf{P}$ taková, že platí $\mathbf{B} = \mathbf{P}^{-1} \cdot \mathbf{A} \cdot \mathbf{P}$.

7.64. Poznámka. Je-li $\mathbf{A}$ podobná $\mathbf{B}$, pak je i $\mathbf{B}$ podobná $\mathbf{A}$, protože místo matice $\mathbf{P}$ můžeme použít matici $\mathbf{P}^{-1}$. Stačí tedy říkat, že matice jsou si vzájemně podobné. Je-li $\mathbf{A}$ podobná $\mathbf{B}$ a $\mathbf{B}$ podobná $\mathbf{C}$, pak je $\mathbf{A}$ podobná $\mathbf{C}$, protože součin regulárních matic je matice regulární a protože $(\mathbf{PQ})^{-1} = \mathbf{Q}^{-1}\mathbf{P}^{-1}$. Matice je podobná sama sobě, protože $\mathbf{E}$ je regulární.

7.65. Poznámka. Následující část textu o vlastních číslech jsem ke kapitole o lineárních zobrazeních zařadil poté, co byla do osnov algebry pro první ročník zařazena zmínka o vlastních vektorech. Je to téma docela rozsáhlé. Zde jsou uvedeny jen základní vlastnosti, takže čtenář s hlubšími zájmy o tuto problematiku bude muset sáhnout po jiném zdroji informací, například [14].

Vlastní číslo, vlastní vektor

7.66. Definice. Nechť $\mathcal{A}: L \to L$ je lineární zobrazení. Číslo $\lambda \in \mathbf{C}$ se nazývá *vlastním číslem zobrazení $\mathcal{A}$*, pokud existuje vektor $\boldsymbol{x} \in L$, $\boldsymbol{x} \neq \boldsymbol{o}$ takový, že $\mathcal{A}(\boldsymbol{x}) = \lambda\,\boldsymbol{x}$. Vektor $\boldsymbol{x}$, který splňuje uvedenou rovnost, se nazývá *vlastní vektor zobrazení $\mathcal{A}$ příslušný vlastnímu číslu λ*.

7.67. Poznámka. Protože vlastní číslo může být číslo komplexní, je potřeba pracovat s modifikovanou definicí lineárního prostoru 1.6, ve které nahradíme množinu reálných čísel množinou čísel komplexních. Jak plyne z definice 7.66, budeme totiž nuceni při práci s vlastními čísly a vlastními vektory násobit vlastní vektor komplexním číslem. V modelových příkladech se pokusím komplexním číslům vyhnout.

7.68. Poznámka. Pokud existuje vlastní číslo zobrazení $\mathcal{A}$, pak mu přísluší více vlastních vektorů. Přidáme-li k těmto vektorům vektor nulový, dostáváme lineární podprostor prostoru L. Skutečně, pokud $\boldsymbol{x}$, $\boldsymbol{y}$ splňují $\mathcal{A}(\boldsymbol{x}) = \lambda\,\boldsymbol{x}$, $\mathcal{A}(\boldsymbol{y}) = \lambda\,\boldsymbol{y}$, pak

$$\mathcal{A}(\boldsymbol{x}+\boldsymbol{y}) = \mathcal{A}(\boldsymbol{x}) + \mathcal{A}(\boldsymbol{y}) = \lambda\,\boldsymbol{x} + \lambda\,\boldsymbol{y} = \lambda\,(\boldsymbol{x}+\boldsymbol{y}), \qquad \mathcal{A}(\alpha\,\boldsymbol{x}) = \alpha\,\mathcal{A}(\boldsymbol{x}) = \alpha\lambda\,\boldsymbol{x} = \lambda\,(\alpha\,\boldsymbol{x}).$$

7.69. Poznámka. Pojem vlastní číslo definujeme nejenom pro lineární zobrazení, ale rovněž pro čtvercové matice. Záhy zjistíme, že mezi vlastním číslem zobrazení a matice je úzká souvislost.

7.70. Definice. Nechť $\mathbf{A}$ je čtvercová matice typu (n,n) reálných nebo komplexních čísel. Číslo $\lambda \in \mathbf{C}$ se nazývá *vlastním číslem matice* $\mathbf{A}$, pokud existuje vektor $\boldsymbol{x} \in \mathbf{C}^n$, $\boldsymbol{x} \neq \boldsymbol{o}$, takový, že $\mathbf{A} \cdot \boldsymbol{x}^T = \lambda\,\boldsymbol{x}^T$. Vektor $\boldsymbol{x}$, který splňuje uvedenou rovnost, se nazývá *vlastní vektor matice* $\mathbf{A}$ *příslušný vlastnímu číslu* λ.

7.71. Věta. Nechť $\mathcal{A}: L \to L$ je lineární zobrazení a $\mathbf{A}$ je jeho matice vzhledem k nějaké bázi (B). Pak λ je vlastním číslem zobrazení $\mathcal{A}$ právě tehdy, když je vlastním číslem matice $\mathbf{A}$. Navíc $\boldsymbol{x}$ je vlastní vektor zobrazení $\mathcal{A}$ příslušný λ právě tehdy, když souřadnice vektoru $\boldsymbol{x}$ vzhledem k bázi (B) tvoří vlastní vektor matice $\mathbf{A}$ příslušný λ.

Důkaz. Označme $\boldsymbol{u} \in \mathbf{C}^n$ souřadnice vektoru $\boldsymbol{x}$ v bázi (B). Podle věty 7.49 sloupec $\mathbf{A} \cdot \boldsymbol{u}^T$ obsahuje souřadnice obrazu $\mathcal{A}(\boldsymbol{x})$ vzhledem k bázi (B). Takže $\mathcal{A}(\boldsymbol{x}) = \lambda\,\boldsymbol{x}$ právě tehdy, když $\mathbf{A} \cdot \boldsymbol{u}^T = \lambda\,\boldsymbol{u}^T$.

7.72. Poznámka. Množina všech vlastních čísel lineárního zobrazení nebo matice se nazývá *spektrum.* Vlastním číslům/vektorům někteří čeští autoři říkají *charakteristická čísla/vektory* (anglicky eigenvalue, eigenvector, což je odvozeno z němčiny).

7.73. Poznámka. Vlastní číslo zobrazení $\mathcal{A}$ je podle předchozí věty vlastním číslem všech matic tohoto zobrazení (vzhledem k rozličným bázím). Tyto matice jsou podle poznámky 7.62 vzájemně podobné. Můžeme tedy říci, že pokud $\mathbf{P}$ je regulární matice, pak vlastní čísla matic $\mathbf{A}$ a $\mathbf{P}^{-1} \cdot \mathbf{A} \cdot \mathbf{P}$ jsou stejná.

7.74. Poznámka. Přikročíme nyní k výpočtu vlastních čísel, je-li dána čtvercová matice $\mathbf{A}$. Vyjdeme z rovnosti $\mathbf{A} \cdot \boldsymbol{x}^T = \lambda\,\boldsymbol{x}^T = \lambda\,\mathbf{E} \cdot \boldsymbol{x}^T$. Z obou stran této rovnice odečteme $\lambda\,\mathbf{E} \cdot \boldsymbol{x}^T$. Dostáváme vztah $\mathbf{A} \cdot \boldsymbol{x}^T - \lambda\,\mathbf{E} \cdot \boldsymbol{x}^T = (\mathbf{A} - \lambda\,\mathbf{E}) \cdot \boldsymbol{x}^T = \boldsymbol{o}^T$. Z definice vlastního čísla víme, že příslušný vlastní vektor $\boldsymbol{x}$ musí být nenulový. Je tedy zřejmé, že λ bude vlastním číslem matice $\mathbf{A}$ právě tehdy, když homogenní soustava s maticí $\mathbf{A} - \lambda\,\mathbf{E}$ bude mít nenulové řešení. Tímto řešením pak bude vlastní vektor příslušný vlastnímu číslu λ. Aby tato soustava měla nenulové řešení, musí její matice být singulární, tj. musí $\det(\mathbf{A} - \lambda\,\mathbf{E}) = 0$. Tím máme odvozen vzorec na výpočet vlastních čísel. Uvědomíme si ještě, že $\det(\mathbf{A} - \lambda\,\mathbf{E})$ je polynom v proměnné λ. Tento polynom se nazývá *charakteristický polynom* matice $\mathbf{A}$. Jeho stupeň je stejný, jako počet řádků matice $\mathbf{A}$. Označme toto číslo n. Abychom tedy našli všechna vlastní čísla dané matice, stačí najít všechny kořeny charakteristického polynomu této matice. Podle základní věty algebry těchto kořenů (včetně jejich násobnosti) je n. Každá matice má tedy n vlastních čísel (obecně ne vzájmeně různých). Každé lineární zobrazení $\mathcal{A}: L \to L$ má tolik vlastních čísel, kolik je dimeze L.

7.75. Definice. Nechť $\mathbf{A}$ je čtvercová matice. Polynom $\det(\mathbf{A} - \lambda\,\mathbf{E})$ nazýváme *charakteristický polynom matice* $\mathbf{A}$ a rovnost $\det(\mathbf{A} - \lambda\,\mathbf{E}) = 0$ charakteristickou rovnicí. Je-li λ k-násobným kořenem charakteristické rovnice, říkáme, že λ je *k-násobným vlastním číslem.*

7.76. Příklad. Uvedeme ještě celý postup odvození výpočtu vlastních čísel matice (viz předchozí poznámku) znovu na konkrétním numerickém příkladě, protože odvození může pro někoho být na konkrétním příkladě názornější. Budeme hledat vlastní čísla a vlastní vektory matice

$$\mathbf{A} = \begin{pmatrix} 5 & -2 & 2 \\ -1 & 4 & -1 \\ -4 & 4 & -1 \end{pmatrix}.$$

Podle definice 7.70 hledáme takové číslo λ a vektor $\boldsymbol{x} = (x_1, x_2, x_3)$, aby byla splněna maticová rovnost

$$\begin{pmatrix} 5 & -2 & 2 \\ -1 & 4 & -1 \\ -4 & 4 & -1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \lambda \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix},$$

a přitom vektor $\boldsymbol{x}$ byl nenulový. Rozepíšeme tuto rovnost do složek:

$$\begin{array}{rcl} 5x_1 - 2x_2 + 2x_3 = \lambda x_1 & & (5-\lambda)x_1 - 2x_2 + 2x_3 = 0 \\ -x_1 + 4x_2 - x_3 = \lambda x_2 & \text{tj.} & -x_1 + (4-\lambda)x_2 - x_3 = 0 \\ -4x_1 + 4x_2 - x_3 = \lambda x_3 & & -4x_1 + 4x_2 + (-1-\lambda)x_3 = 0 \end{array}$$

Potřebujeme, aby uvedená homogenní soustava se čtvercovou maticí měla nenulové řešení. Matice soustavy tedy musí být singulární, tj. musí mít nulový determinant:

$$\det \begin{pmatrix} 5-\lambda & -2 & 2 \\ -1 & 4-\lambda & -1 \\ -4 & 4 & -1-\lambda \end{pmatrix} = 0.$$

Hledáme tedy λ takové, aby $\det(\mathbf{A}-\lambda\mathbf{E})=0$. Příště už toto odvození nebudeme opakovat, ale začneme rovnou od rovnice $\det(\mathbf{A}-\lambda\mathbf{E})=0$.

$$\det(\mathbf{A}-\lambda\mathbf{E})=(5-\lambda)(4-\lambda)(-1-\lambda)-16-\big(-4(4-\lambda)-4(5-\lambda)+2(-1-\lambda)\big)=-(\lambda-3)^2(\lambda-2),$$

takže vlastní čísla jsou $\lambda=3$ a $\lambda=2$. Najdeme ještě vlastní vektory. Nejprve najdeme vlastní vektory příslušné vlastnímu číslu 3:

$$\begin{pmatrix} 5-3 & -2 & 2 \\ -1 & 4-3 & -1 \\ -4 & 4 & -1-3 \end{pmatrix} = \begin{pmatrix} 2 & -2 & 2 \\ -1 & 1 & -1 \\ -4 & 4 & -4 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & 1 \end{pmatrix}.$$

Báze řešení homogenní soustavy s maticí $(1\ -1\ \ 1)$ je například $\{(1,1,0),(-1,0,1)\}$. Toto jsou dva lineárně nezávislé vlastní vektory, které přísluší vlastnímu číslu 3. Všechny vlastní vektory příslušející vlastnímu číslu 3 tvoří lineární obal této báze, ovšem bez nulového vektoru. Nyní najdeme vlastní vektory, které přísluší vlastnímu číslu 2:

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

Dimenze prostoru řešení homogenní soustavy s touto maticí je 1, tj. stačí najít jeden vektor řešení: $(-2,1,4)$ a ostatní vektory řešení jsou jeho násobky. Tato řešení (bez nulového) jsou též všechny vlastní vektory matice $\mathbf{A}$, které přísluší vlastnímu číslu 2.

Celkem tedy má matice $\mathbf{A}$ tři lineárně nezávislé vlastní vektory: $(1,1,0),(-1,0,1),(-2,1,4)$. První dva příslušejí vlastnímu číslu 3 a poslední přísluší vlastnímu číslu 2.

7.77. Příklad. Následující příklad ukazuje, že nemusí existovat tolik lineárně nezávislých vlastních vektorů, kolik řádků má matice. Budeme hledat vlastní čísla a vlastní vektory matice:

$$\mathbf{A}=\begin{pmatrix} 2 & 4 & -3 \\ -1 & 10 & -6 \\ -1 & 8 & -4 \end{pmatrix}.$$

Vypočteme determinant matice $\mathbf{A}-\lambda\mathbf{E}$:

$$\det\begin{pmatrix} 2-\lambda & 4 & -3 \\ -1 & 10-\lambda & -6 \\ -1 & 8 & -4-\lambda \end{pmatrix} = -(\lambda-3)^2(\lambda-2).$$

Vidíme, že matice má stejná vlastní čísla, jako matice z předchozího příkladu. Nyní vypočítáme vlastní vektory:

$$\lambda=3:\quad \begin{pmatrix} 2-3 & 4 & -3 \\ -1 & 10-3 & -6 \\ -1 & 8 & -4-3 \end{pmatrix} = \begin{pmatrix} -1 & 4 & -3 \\ -1 & 7 & -6 \\ -1 & 8 & -7 \end{pmatrix} \sim \begin{pmatrix} -1 & 4 & -3 \\ 0 & 3 & -3 \\ 0 & 4 & -4 \end{pmatrix} \sim \begin{pmatrix} -1 & 4 & -3 \\ 0 & 1 & -1 \end{pmatrix} \quad \begin{matrix}\text{vlastní}\\ \text{vektor:}\\ (1,1,1)\end{matrix}$$

$$\lambda=2:\quad \begin{pmatrix} 2-2 & 4 & -3 \\ -1 & 10-2 & -6 \\ -1 & 8 & -4-2 \end{pmatrix} = \begin{pmatrix} 0 & 4 & -3 \\ -1 & 8 & -6 \\ -1 & 8 & -6 \end{pmatrix} \sim \begin{pmatrix} -1 & 8 & -6 \\ 0 & 4 & -3 \end{pmatrix} \quad \begin{matrix}\text{vlastní}\\ \text{vektor:}\\ (0,3,4)\end{matrix}$$

Na rozdíl od předchozího příkladu vícenásobnému vlastnímu číslu 3 přísluší jen jeden lineárně nezávislý vlastní vektor. Tato matice má tedy dohromady jen dva lineárně nezávislé vlastní vektory: $(1,1,1),(0,3,4)$, které po řadě příslušejí vlastním číslům 3 a 2.

7.78. Věta. Podobné matice mají stejný charakteristický polynom.

Důkaz. Nechť $\mathbf{P}$ je regulární. Matice $\mathbf{P}^{-1}\mathbf{A}\mathbf{P}$ je podobná matici $\mathbf{A}$. Vypočteme její charakteristický polynom:

$$\begin{aligned}\det(\mathbf{P}^{-1}\mathbf{A}\mathbf{P}-\lambda\,\mathbf{E}) &= \det(\mathbf{P}^{-1}\mathbf{A}\mathbf{P}-\lambda\,\mathbf{P}^{-1}\mathbf{E}\mathbf{P}) = \det(\mathbf{P}^{-1}\mathbf{A}\mathbf{P}-\mathbf{P}^{-1}\lambda\,\mathbf{E}\mathbf{P}) = \\ &= \det(\mathbf{P}^{-1}\,(\mathbf{A}-\lambda\,\mathbf{E})\,\mathbf{P}) = \det\mathbf{P}^{-1}\,\det(\mathbf{A}-\lambda\,\mathbf{E})\,\det\mathbf{P} = \det(\mathbf{A}-\lambda\,\mathbf{E}),\end{aligned}$$

protože $\det\mathbf{P}^{-1}\det\mathbf{P}=1$.

7.79. Poznámka. Právě uvedený výsledek je v souladu s poznámkou 7.73.

7.80. Poznámka. Matice z příkladů 7.76 a 7.77 mají sice stejný charakteristický polynom, ale za chvíli ukážeme, že si nejsou podobné. Tvrzení věty 7.78 tedy nelze obrátit.

7.81. Příklad. Diagonální matice

Podobnost s diagonální maticí

$$\mathbf{D} = \begin{pmatrix} \lambda_1 & 0 & 0 & \dots & 0 \\ 0 & \lambda_2 & 0 & \dots & 0 \\ 0 & 0 & \lambda_3 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

má charakteristický polynom $(\lambda_1 - \lambda)\,(\lambda_2 - \lambda) \cdots (\lambda_n - \lambda)$, protože determinant diagonální matice $\mathbf{D} - \lambda\,\mathbf{E}$ je roven součinu prvků na diagonále. Vlastní čísla matice $\mathbf{D}$ tedy jsou $\lambda_1, \lambda_2, \dots, \lambda_n$.

Vlastní vektor matice $\mathbf{D}$ příslušný vlastnímu číslu λ_i je vektor obsahující samé nuly s výjimkou i-té složky, ve které je nějaké nenulové číslo, třeba jednička.

Matici $\mathbf{D}$ z tohoto příkladu budeme značit $\mathbf{D} = \operatorname{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$. Tím ušetříme papír.

7.82. Věta. Nechť $\mathbf{A}$ je čtvercová matice typu (n, n). Sestavme libovolná komplexní čísla $\lambda_1, \dots, \lambda_n$ do diagonální matice $\mathbf{D} = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$ a libovolné nenulové vektory $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ z $\mathbf{C}^n$ zapišme do sloupců matice $\mathbf{P}$, tj. $\mathbf{P} = (\boldsymbol{x}_1^T, \dots, \boldsymbol{x}_n^T)$. Pak platí: čísla $\lambda_1, \dots, \lambda_n$ jsou vlastními čísly matice $\mathbf{A}$ a $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ jsou jejich odpovídající vlastní vektory právě tehdy, když je splněna rovnost $\mathbf{PD} = \mathbf{AP}$.

Důkaz. Rozepišme maticové násobení: $\mathbf{PD} = (\boldsymbol{x}_1^T, \dots, \boldsymbol{x}_n^T) \cdot \operatorname{diag}(\lambda_1, \dots, \lambda_n) = (\lambda_1\,\boldsymbol{x}_1^T, \dots, \lambda_n\,\boldsymbol{x}_n^T)$. Dále je $\mathbf{AP} = \mathbf{A}(\boldsymbol{x}_1^T, \dots, \boldsymbol{x}_n^T) = (\mathbf{A}\boldsymbol{x}_1^T, \dots, \mathbf{A}\boldsymbol{x}_1^T)$. Máme tedy obě strany zkoumané rovnosti $\mathbf{PD} = \mathbf{AP}$ rozepsány do sloupců. Vidíme, že rovnost v i-tém sloupci $\lambda_i\,\boldsymbol{x}_i^T = \mathbf{A}\boldsymbol{x}_i^T$ platí právě tehdy, když λ_i je vlastní číslo matice $\mathbf{A}$ a $\boldsymbol{x}_i$ je příslušný vlastní vektor.

7.83. Věta. Nechť má čtvercová matice $\mathbf{A}$ s n řádky n lineárně nezávislých vlastních vektorů (každý z nich přísluší nějakému vlastnímu číslu matice). Pak je matice $\mathbf{A}$ podobná diagonální matici.

Důkaz. Sestavíme diagonální matici $\mathbf{D}$ z vlastních čísel příslušných vlastním vektorům $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$. Dále použijeme předchozí větu. Protože matice $\mathbf{P} = (\boldsymbol{x}_1^T, \dots, \boldsymbol{x}_n^T)$ obsahuje podle předpokladu věty lineárně nezávislé sloupce, je $\mathbf{P}$ regulární, takže je možné vztah $\mathbf{PD} = \mathbf{AP}$ vynásobit zprava maticí $\mathbf{P}^{-1}$. Dostáváme $\mathbf{A} = \mathbf{PDP}^{-1}$, takže matice $\mathbf{A}$ je podobná matici $\mathbf{D}$.

7.84. Věta. Nechť je matice $\mathbf{A}$ podobná diagonální matici, to znamená, že existuje regulární matice $\mathbf{P}$ a diagonální matice $\mathbf{D}$ takové, že $\mathbf{A} = \mathbf{PDP}^{-1}$. Pak $\mathbf{D}$ obsahuje vlastní čísla matice $\mathbf{A}$ a ve sloupcích matice $\mathbf{P}$ jsou vlastní vektory příslušné (podle pořadí) odpovídajícím vlastním číslům zapsaným v $\mathbf{D}$.

Důkaz. Po převedení vztahu $\mathbf{A} = \mathbf{PDP}^{-1}$ na $\mathbf{AP} = \mathbf{PD}$ stačí použít větu 7.82.

7.85. Příklad. Matice z příkladu 7.76 má tři řádky a tři lineárně nezávislé vlastní vektory. Jsou tedy splněny předpoklady věty 7.83 a matice je podobná diagonální matici. Věta 7.84 nám dává návod, jak najít matici $\mathbf{P}$ a diagonální matici. Sestavíme vlastní vektory $(1, 1, 0), (-1, 0, 1), (-2, 1, 4)$ do sloupců a dostáváme matici $\mathbf{P}$. Sestavíme v odpovídajícím pořadí vlastní čísla do diagonální matice, a dostáváme matici $\mathbf{D}$, pro kterou platí $\mathbf{A} = \mathbf{PDP}^{-1}$. Konkrétně:

$$\mathbf{A} = \begin{pmatrix} 5 & -2 & 2 \\ -1 & 4 & -1 \\ -4 & 4 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 & -2 \\ 1 & 0 & 1 \\ 0 & 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & -2 \\ 1 & 0 & 1 \\ 0 & 1 & 4 \end{pmatrix}^{-1}.$$

7.86. Příklad. Matice z příkladu 7.77 nemá tolik lineárně nezávislých vlastních vektorů, jako je počet jejích řádků. To znamená, že není podobná diagonální matici (kdyby byla, pak dostaneme spor s větou 7.84. Protože matice z příkladu 7.76 je podobná diagonální matici, zatímco matice z příkladu 7.77 není, nejsou si tyto matice ani vzájemně podobné.

7.87. Věta. Vlastní vektory, které příslušejí vzájemně různým vlastním číslům, jsou lineárně nezávislé.

Důkaz. Jeden vlastní vektor je samozřejmě lineárně nezávislý, protože je podle definice nenulový. Dále postupujeme indukcí. Přepokládáme, že matice $\mathbf{A}$ má lineárně nezávislé vlastní vektory $\boldsymbol{x}_1, \dots \boldsymbol{x}_k$ příslušející různým vlastním číslům $\lambda_1, \dots, \lambda_k$ a přidáme do této skupiny vlastní vektor $\boldsymbol{x}_{k+1}$ příslušející zatím nepoužitému vlastnímu číslu λ_{k+1}. Předpokládáme rovnost $\sum_{i=1}^{k+1} \alpha_i \boldsymbol{x}_i = \boldsymbol{o}$ a ukážeme, že všechny koeficienty α_i musejí být nulové. Tím dokážeme lineární nezávislost. Rovnost transponujeme a vynásobíme zleva maticí $\mathbf{A} - \lambda_{k+1}\mathbf{E}$. Dostáváme:

$$(\mathbf{A} - \lambda_{k+1}\mathbf{E}) \sum_{i=1}^{k+1} \alpha_i \boldsymbol{x}_i^T = \sum_{i=1}^{k+1} \alpha_i (\mathbf{A}\boldsymbol{x}_i^T - \lambda_{k+1}\boldsymbol{x}_i^T) = \sum_{i=1}^{k+1} \alpha_i (\lambda_i \boldsymbol{x}_i^T - \lambda_{k+1}\boldsymbol{x}_i^T) = \sum_{i=1}^{k+1} \alpha_i (\lambda_i - \lambda_{k+1})\, \boldsymbol{x}_i^T = \boldsymbol{o}^T.$$

Koeficient u posledního sčítance v této rovnosti je nulový, protože $\lambda_{k+1} - \lambda_{k+1} = 0$. Podle indukčního předpokladu jsou vektory $\boldsymbol{x}_1, \dots \boldsymbol{x}_k$ lineárně nezávislé, takže i ostatní koeficienty musejí být nulové. Protože ale $\lambda_i \neq \lambda_{k+1}$, musí $\alpha_i = 0$ pro $i \in \{1, \dots, k\}$. Dosadíme-li tento poznatek do výchozího tvaru rovnosti, máme $0\,\boldsymbol{x}_1 + \cdots + 0\,\boldsymbol{x}_k + \alpha_{k+1}\boldsymbol{x}_{k+1} = \alpha_{k+1}\boldsymbol{x}_{k+1} = \boldsymbol{o}$. Protože $\boldsymbol{x}_{k+1}$ je vlastní vektor a tudíž nenulový, musí $\alpha_{k+1} = 0$.

7.88. Poznámka. Nechť $\mathbf{A}$ je typu (n, n) a nechť jsou všechna vlastní čísla matice $\mathbf{A}$ jednonásobná. To znamená, že existuje n různých vlastních čísel. Pak podle předchozí věty jim příslušející vlastní vektory jsou lineárně nezávislé. Podle věty 7.83 je tedy matice $\mathbf{A}$ podobná diagonální matici.

7.89. Poznámka. Uvažujme matici $\mathbf{A}$ typu (n, n). Může se stát, že nějaké vlastní číslo λ této matice je vícenásobné. To může ale nemusí způsobit, že k matici $\mathbf{A}$ přestane existovat podobná diagonální matice. Záleží na čísle $d_\lambda = n - \mathrm{hod}(\mathbf{A} - \lambda\mathbf{E})$. Protože $\mathbf{A} - \lambda\mathbf{E}$ je singulární, je toto číslo aspoň 1. Vzhledem k tomu, že d_λ je dimenze prostoru řešení homogenní soustavy $(\mathbf{A} - \lambda\mathbf{E})\,\boldsymbol{x} = \boldsymbol{o}$, můžeme najít k vlastnímu číslu λ právě d_λ lineárně nezávislých vlastních vektorů. Prostudujeme-li zpětně důkaz věty 7.87, shledáme, že jsme v indukčním kroku nepotřebovali vzájemnou různost vlastních čísel $\lambda_1, \dots, \lambda_k$, jen jsme chtěli, aby λ_{k+1} bylo od ostatních různé. Pokud je číslo d_λ pro každé vícenásobné vlastní číslo rovno jeho násobnosti, pak můžeme postupně do „balíčku linárně nezávislých vlastních vektorů“ přihazovat za každé vlastní číslo tolik vektorů, kolik je násobnost vlastního čísla. Dohromady získáme n lineárně nezávislých vektorů, takže podle věty 7.83 je $\mathbf{A}$ podobná diagonální matici.

7.90. Poznámka. Stále předpokládáme čtvercovou matici $\mathbf{A}$ typu (n, n). Problémy nastanou, pokud číslo $d_\lambda = n - \mathrm{hod}(\mathbf{A} - \lambda\mathbf{E})$ je menší než násobnost vlastního čísla λ. Pak nelze najít n lineárně nezávislých vlastních vektorů a matice $\mathbf{A}$ není podobná diagonální matici. Příklad 7.77 ilustruje, že takové případy opravdu nastávají. Matice $\mathbf{A}$ je pak podobná jen „skoro diagonální matici“, která má na hlavní diagonále vlastní čísla a těsně nad touto diagonálou se občas vyskytují jedničky. Této matici se říká *Jordanův kanonický tvar*. Je potřeba definovat tzv. *zobecněný vlastní vektor* a tento pojem použít k vybudování regulární matice $\mathbf{P}$, která převádí matici $\mathbf{A}$ na Jordanův kanonický tvar. Všechny tyto pojmy vyžadují hlubší studium a přesahují bohužel rámec tohoto úvodního textu. Pro další studium lze doporučit [14].

7.91. Poznámka. Věty 7.83 a 7.84 se dají formulovat z úhlu pohledu lineárního zobrazení:

7.92. Věta. Nechť $\mathcal{A}\colon L \to L$ je lineární zobrazení, $\dim L = n$. Zobrazení $\mathcal{A}$ má n lineárně nezávislých vlastních vektorů právě tehdy, když existuje báze (B) prostoru L taková, že $\mathcal{A}$ má vzhledem k této bázi diagonální matici $\mathbf{D}$. Přitom na diagonále matice $\mathbf{D}$ jsou vlastní čísla zobrazení $\mathcal{A}$ a báze (B) obsahuje vlastní vektory příslušné vlastním číslům v matici $\mathbf{D}$ ve stejném pořadí.

Důkaz. Zvolme nějakou výchozí bázi (V) prostoru L. Označme symbolem $\mathbf{A}$ matici zobrazení $\mathcal{A}$ vzhledem k bázi (V). Existence báze (B) takové, že matice zobrazení $\mathcal{A}$ vzhledem k ní je $\mathbf{D}$, je ekvivalentní s platností vztahu $\mathbf{A} = \mathbf{P}\mathbf{D}\mathbf{P}^{-1}$, kde $\mathbf{P}$ je matice přechodu od (V) k (B). Dále při důkazu tvrzení „právě tehdy když“ použijeme v jednom směru větu 7.83. V druhém směru použijeme větu 7.84 a skutečnost, že matice přechodu $\mathbf{P}$ obsahuje ve sloupcích souřadnice báze (B) vzhledem k bázi (V).

7.93. Poznámka. Při práci s lineárním zobrazením se někdy hodí zvolit takovou bázi, ve které je matice tohoto zobrazení „co nejbližší“ matici diagonální. Právě vyslovená věta říká, že za jistých okolností lze zvolit bázi, vzhledem ke které je matice zobrazení přímo diagonální. Pokud $(x_1, \dots, x_n)$ jsou souřadnice vstupního vektoru $\boldsymbol{x}$ vzhledem k této bázi, pak výstupní vektor $\mathcal{A}(\boldsymbol{x})$ má vzhledem ke stejné bázi souřadnice $(\lambda_1 x_1, \dots, \lambda_n x_n)$, kde $\lambda_1, \dots, \lambda_n$ jsou vlastní čísla tohoto zobrazení.

8. Lineární prostory se skalárním součinem

8.1. Poznámka. Lineární prostor je libovolná množina, na které je definováno sčítání a násobení konstantou tak, aby byly splněny vlastnosti (1) až (7) z definice 1.6. Pokud na takové množině navíc definujeme násobení prvků *mezi sebou* tak, že výsledek násobení je reálné číslo a násobení splňuje níže uvedené vlastnosti (1) až (4), definovali jsme na lineárním prostoru skalární součin. Ten nám umožní pracovat s novými vlastnostmi prvků lineárního prostoru, jako je jejich velikost a úhel mezi dvěma prvky.

8.2. Definice. Nechť L je lineární prostor. Operaci $\cdot : L \times L \to \mathbf{R}$ nazveme *skalárním součinem*, pokud splňuje $\forall \boldsymbol{x} \in L$, $\forall \boldsymbol{y} \in L$, $\forall \boldsymbol{z} \in L$, $\forall \alpha \in \mathbf{R}$ následující vlastnosti

Definice skalárního součinu

$$
\begin{aligned}
&(1) \quad \boldsymbol{x} \cdot \boldsymbol{y} = \boldsymbol{y} \cdot \boldsymbol{x},\\
&(2) \quad (\boldsymbol{x} + \boldsymbol{y}) \cdot \boldsymbol{z} = \boldsymbol{x} \cdot \boldsymbol{z} + \boldsymbol{y} \cdot \boldsymbol{z},\\
&(3) \quad (\alpha \cdot \boldsymbol{x}) \cdot \boldsymbol{y} = \alpha \cdot (\boldsymbol{x} \cdot \boldsymbol{y}),\\
&(4) \quad \boldsymbol{x} \cdot \boldsymbol{x} \geq 0, \quad \boldsymbol{x} \cdot \boldsymbol{x} = 0 \text{ jen tehdy, když } \boldsymbol{x} = \boldsymbol{o}.
\end{aligned}
$$

Ve vlastnosti (4) značí symbol $\boldsymbol{o}$ nulový vektor lineárního prostoru L.

Lineární prostor L, na kterém je definován skalární součin, nazýváme *lineárním prostorem se skalárním součinem.*

8.3. Poznámka. Je třeba rozlišovat mezi podobně znějícími pojmy „skalární násobek“ a „skalární součin“. Skalární násobek $\cdot : \mathbf{R} \times L \to L$ je násobek vektoru reálným číslem, který je definován v každém lineárním prostoru. Na druhé straně skalární součin $\cdot : L \times L \to \mathbf{R}$ je součin vektorů mezi sebou.

8.4. Poznámka. Upozorňujeme, že stejně jako v definici lineárního prostoru 1.6, jsou ve vlastnostech (1) až (4) definice skalárního součinu používány symboly „+“ a „·“ v různých významech podle toho, jakého typu jsou jejich operandy. Například první „+“ ve vlastnosti (2) označuje sčítání vektorů podle definice lineárního prostoru, zatímco druhé „+“ v této vlastnosti je sčítáním reálných čísel. Nebo první symbol „·“ ve vlastnosti (3) znamená skalární násobek definovaný v lineárním prostoru L, druhý symbol „·“ označuje skalární součin. Třetí symbol „·“ ve vlastnosti (3) je součin reálných čísel a poslední symbol „·“ v této vlastnosti znovu znamená skalární součin.

Dále připomínáme, že budeme symbol „·“ jako dosud často vynechávat, takže místo $\boldsymbol{x} \cdot \boldsymbol{y}$ budeme stručně psát $\boldsymbol{xy}$.

8.5. Poznámka. Všimneme si, že jsme v definici 1.6 lineárního prostoru definovali tento prostor „nad reálnými čísly“, protože jsme definovali násobek vektoru *reálným číslem.* Nic nám ale nebránilo zcela stejně definovat násobek vektoru komplexním číslem. Až dosud jsme mohli nahradit slovo „reálné číslo“ slovem „komplexní číslo“ a naše teorie by zůstala platná. Všechny předchozí věty by nadále platily.

Kdybychom ale chtěli definovat skalární součin jako komplexní číslo, museli bychom upravit vlastnost (1) definice 8.2 takto:

$$(1) \quad \boldsymbol{xy} = \overline{\boldsymbol{yx}},$$

kde pruh nad komplexním číslem $\boldsymbol{yx}$ značí komplexně sdružené číslo. Některá tvrzení se tedy budou v případě komplexního skalárního součinu nepatrně lišit od tvrzení, která níže dokážeme. Protože se většina čtenářů tohoto textu nachází zatím v prvním semestru a nemá za sebou analýzu komplexních čísel, zjednodušíme si život tím, že zůstaneme u reálných čísel. Pro odvození důležitých vlastností lineárních prostorů se skalárním součinem nám to bude stačit. Zájemce o důsledky definice komplexního skalárního součinu odkážeme například na učebnici [5].

8.6. Věta. Nechť L je lineární prostor se skalárním součinem, $\boldsymbol{o}$ je jeho nulový vektor. Pak pro všechna $\boldsymbol{x} \in L$, $\boldsymbol{y} \in L$ a $\boldsymbol{z} \in L$ platí: (1) $\boldsymbol{x} \cdot \boldsymbol{o} = \boldsymbol{o} \cdot \boldsymbol{x} = 0$, (2) $\boldsymbol{z} \cdot (\boldsymbol{x} + \boldsymbol{y}) = \boldsymbol{zx} + \boldsymbol{zy}$.

Důkaz. První vlastnost plyne z vlastnosti (7) definice lineárního prostoru 1.6 a z vlastnosti (3) definice skalárního součinu 8.2. Platí $(0\boldsymbol{y}) \cdot \boldsymbol{x} = 0 \cdot \boldsymbol{xy} = 0$

Druhá vlastnost plyne z komutativity skalárního součinu, tj. z vlastnosti (1) definice 8.2 a dále z vlastnosti (2) této definice.

8.7. Příklad. Pro $\boldsymbol{x} \in \mathbf{R}^n$, $\boldsymbol{y} \in \mathbf{R}^n$, $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$, $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$ definujme

Skalární součiny na $\mathbf{R}^n$

$$\boldsymbol{x} \cdot \boldsymbol{y} = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n. \tag{8.1}$$

Ukážeme, že takto definovaný součin vektorů $\boldsymbol{x}$ a $\boldsymbol{y}$ je skalárním součinem. Je $\boldsymbol{x} \cdot \boldsymbol{y} \in \mathbf{R}$. Nechť ještě $\boldsymbol{z} \in \mathbf{R}^n$, $\boldsymbol{z} = (z_1, z_2, \ldots, z_n)$ a $\alpha \in \mathbf{R}$. Ověříme postupně vlastnosti (1) až (4):

$$
\begin{aligned}
&(1) \quad \boldsymbol{x} \cdot \boldsymbol{y} = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n = y_1 x_1 + y_2 x_2 + \cdots + y_n x_n = \boldsymbol{y} \cdot \boldsymbol{x},\\
&(2) \quad (\boldsymbol{x} + \boldsymbol{y}) \cdot \boldsymbol{z} = (x_1 + y_1)\, z_1 + (x_2 + y_2)\, z_2 + \cdots + (x_n + y_n)\, z_n =\\
&\qquad = x_1 z_1 + x_2 z_2 + \cdots + x_n z_n + y_1 z_1 + y_2 z_2 + \cdots + y_n z_n = \boldsymbol{x} \cdot \boldsymbol{z} + \boldsymbol{y} \cdot \boldsymbol{z},\\
&(3) \quad (\alpha \cdot \boldsymbol{x}) \cdot \boldsymbol{y} = \alpha x_1 y_1 + \alpha x_2 y_2 + \cdots + \alpha x_n y_n = \alpha\,(x_1 y_1 + x_2 y_2 + \cdots + x_n y_n) = \alpha\,(\boldsymbol{x} \cdot \boldsymbol{y}),\\
&(4) \quad \boldsymbol{x} \cdot \boldsymbol{x} = x_1^2 + x_2^2 + \cdots + x_n^2 \geq 0.
\end{aligned}
$$

Vidíme, že z $x_1^2 + x_2^2 + \cdots + x_n^2 = 0$ plyne $x_1 = x_2 = \cdots = x_n = 0$, takže je splněna i druhá část vlastnosti (4).

Skalární součin na $\mathbf{R}^n$ definovaný vzorcem (8.1) nazýváme *standardním skalárním součinem.* Následující příklady ukazují, že existují i jiné skalární součiny na $\mathbf{R}^n$.

8.8. Příklad. Definujme součin na $\mathbf{R}^2$ takto

$$(x_1, x_2) \cdot (y_1, y_2) = x_1 y_1 + 6 x_2 y_2 + 2 x_1 y_2 + 2 x_2 y_1.$$

Ukážeme, že takto definovaný součin je skalárním součinem na $\mathbf{R}^2$.

Ověříme vlastnosti (1) až (4) definice 8.2

$$
\begin{aligned}
&(1) \quad (x_1, x_2) \cdot (y_1, y_2) = x_1 y_1 + 6 x_2 y_2 + 2 x_1 y_2 + 2 x_2 y_1 =\\
&\qquad = y_1 x_1 + 6 y_2 x_2 + 2 y_1 x_2 + 2 y_2 x_1 = (y_1, y_2) \cdot (x_1, x_2),\\
&(2) \quad \big((x_1, x_2) + (y_1, y_2)\big) \cdot (z_1, z_2) = (x_1 + y_1)\, z_1 + 6(x_2 + y_2)\, z_2 + 2(x_1 + y_1)\, z_2 + 2(x_2 + y_2)\, z_1 =\\
&\qquad = x_1 z_1 + 6 x_2 z_2 + 2 x_1 z_2 + 2 x_2 z_1 + y_1 z_1 + 6 y_2 z_2 + 2 y_1 z_2 + 2 y_2 z_1 =\\
&\qquad = (x_1, x_2) \cdot (z_1, z_2) + (y_1, y_2) \cdot (z_1, z_2),\\
&(3) \quad \big(\alpha\,(x_1, x_2)\big) \cdot (y_1, y_2) = (\alpha\, x_1, \alpha\, x_2) \cdot (y_1, y_2) = \alpha x_1 y_1 + 6 \alpha x_2 y_2 + 2 \alpha x_1 y_2 + 2 \alpha x_2 y_1 =\\
&\qquad = \alpha\,(x_1 y_1 + 6 x_2 y_2 + 2 x_1 y_2 + 2 x_2 y_1) = \alpha\,\big((x_1, x_2) \cdot (y_1, y_2)\big),\\
&(4) \quad (x_1, x_2) \cdot (x_1, x_2) = x_1^2 + 6 x_2^2 + 4 x_1 x_2 \overset{?}{\geq} 0.
\end{aligned}
$$

Abychom dokázali vlastnost (4), potřebujeme pro $x_1 \neq 0$, $x_2 \neq 0$ dokázat, že $x_1^2 + 6x_2^2 + 4x_1 x_2 > 0$. Nechť $a = x_2/x_1$, tj. $x_2 = a x_1$. Po dosazení je $x_1^2 + 6a^2 x_1^2 + 4a x_1^2 = x_1^2(1 + 6a^2 + 4a)$. Aby byl daný výraz větší než nula, stačí aby $6a^2 + 4a + 1 > 0$, $\forall a \in \mathbf{R}$. Protože diskriminant této kvadratické nerovnice je roven $D = 16 - 24 = -8 < 0$, je nerovnost $6a^2 + 4a + 1 > 0$ splněna pro všechna $a \in \mathbf{R}$.

8.9. Příklad. Ukážeme, že předpis $(x_1, x_2) \circ (y_1, y_2) = x_1 y_1 + 2 x_2 y_2 + 2 x_1 y_2 + 2 x_2 y_1$ není skalárním součinem. Vlastnosti (1) až (3) jsou zřejmě splněny. Není splněna vlastnost (4), protože například

$$(-1, 1) \circ (-1, 1) = 1 + 2 - 2 - 2 = -1 \not\geq 0.$$

8.10. Poznámka. Výše uvedené příklady nás vedou k otázce, jak charakterizovat všechny skalární součiny na $\mathbf{R}^n$ a jak je rychle poznat. Souvisí to s tzv. pozitivně definitními a symetrickými maticemi. Níže uvádím nejdůležitější výsledky z této oblasti jen pro čtenáře, který chce být lépe informován. Nám ostatním bude v dalším textu stačit existence standardního skalárního součinu na $\mathbf{R}^n$ a povědomí, že existují i jiné skalární součiny. Téma symetrických a pozitivně definitních matic je možno přeskočit a věnovat se rovnou definici velikosti vektoru 8.17.

Symetrické a pozitivně definitní matice

8.11. Definice. Čtvercová matice $\mathbf{A}$ typu (n, n) je *symetrická*, pokud platí $\mathbf{A}^T = \mathbf{A}$.

8.12. Definice. Nechť $\mathbf{A}$ je čtvercová matice typu (n, n). Označme $\mathbf{A}_i$ čtvercovou matici typu $(n-i, n-i)$, která vzniká z matice $\mathbf{A}$ vynecháním posledních i řádků a posledních i sloupců. Matice $\mathbf{A}$ se nazývá *pozitivně definitní*, pokud všechny determinanty $\det \mathbf{A}_i$, $i \in \{0, 1, 2, \ldots, n-1\}$ jsou kladné.

8.13. Poznámka. Pozitivně definitní matice je vždy regulární, protože $\det \mathbf{A} = \det \mathbf{A}_0 > 0$.

8.14. Věta. Nechť $\mathbf{A}$ je čtvercová matice typu (n, n). Definujme součin na $\mathbf{R}^n$ takto. Pro $\boldsymbol{x} \in \mathbf{R}^n$, $\boldsymbol{y} \in \mathbf{R}^n$ je

$$\boldsymbol{x} \cdot \boldsymbol{y} = \boldsymbol{x} \cdot \mathbf{A} \cdot \boldsymbol{y}^T,$$

kde na pravé straně rovnosti je maticový součin jednořádkové matice $\boldsymbol{x}$, která obsahuje složky vektoru $\boldsymbol{x}$, s maticí $\mathbf{A}$ a s maticí $\boldsymbol{y}^T$, což je sloupec složek vektoru $\boldsymbol{y}$.

Pak $\boldsymbol{x} \cdot \boldsymbol{y}$ je skalárním součinem právě tehdy, když $\mathbf{A}$ je symetrická a pozitivně definitní matice.

Důkaz. Uvedeme jen stručný náznak. Pro vlastnost (1) skalárního součinu je nutná symetrie matice $\mathbf{A}$. Vlastnost (2) a (3) je zaručena pro jakoukoli čtvercovou matici $\mathbf{A}$. Konečně vlastnost (4) je zaručena díky tomu, že matice $\mathbf{A}$ je pozitivně definitní. Na oprávněnou otázku „proč“ zde máme malý prostor pro odpověď. Odkazujeme například na učebnici [5].

8.15. Příklad. Vraťme se k příkladu 8.8. Tam je skalární součin definován takto:

$$\boldsymbol{x} \cdot \boldsymbol{y} = (x_1, x_2) \cdot \begin{pmatrix} 1 & 2 \\ 2 & 6 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

Protože pro uvedenou matici platí $\mathbf{A} = \mathbf{A}^T$, jedná se o symetrickou matici. Spočteme dále jednotlivé determinanty: $\det \mathbf{A}_0 = \det \mathbf{A} = 2$, $\det \mathbf{A}_1 = \det(1) = 1$. Protože oba determinanty jsou kladná čísla, jedná se o pozitivně definitní matici. Podle věty 8.14 je definovaný součin skalárním součinem.

8.16. Poznámka. Budeme definovat velikost vektoru a úhel mezi dvěma nenulovými vektory na obecných lineárních prostorech se skalárním součinem. Tyto pojmy definujeme jen pomocí skalárního součinu pro zcela libovolné vektory. V následující kapitole ukážeme, že pokud budeme pracovat s vektory s geometrickým významem (např. s orientovanými úsečkami), pak pojmy velikost a úhel nyní zavedené abstraktně budou znamenat přesně to, co od nich z geometrického hlediska očekáváme. *Velikost vektoru*

8.17. Definice. Nechť L je lineární prostor se skalárním součinem. Pro $\boldsymbol{x} \in L$ definujeme *velikost vektoru* $\boldsymbol{x}$ hodnotou $\sqrt{\boldsymbol{x} \cdot \boldsymbol{x}}$. Velikost vektoru $\boldsymbol{x}$ značíme $\|\boldsymbol{x}\|$, takže je

$$\|\boldsymbol{x}\| = \sqrt{\boldsymbol{x} \cdot \boldsymbol{x}}, \qquad \text{tj.} \ \ \|\boldsymbol{x}\|^2 = \boldsymbol{x} \cdot \boldsymbol{x}.$$

Místo pojmu „velikost vektoru“ se často používá pojem *norma vektoru.*

8.18. Poznámka. Vidíme, že velikost je nezáporné číslo a že každý vektor má svou velikost. To nám zaručuje vlastnost (4) definice 8.2. Je $\boldsymbol{x} \cdot \boldsymbol{x} \ge 0$, takže odmocnina z tohoto čísla je definována.

Dále vidíme, že jedině nulový vektor má velikost rovnu nule a žádný jiný. To nám zaručuje druhá část vlastnosti (4).

8.19. Věta. Nechť $\boldsymbol{x}$ je prvkem lineárního prostoru se skalárním součinem, $\alpha \in \mathbf{R}$. Pak

$$\|\alpha\, \boldsymbol{x}\| = |\alpha| \cdot \|\boldsymbol{x}\|.$$

Důkaz. $\|\alpha\, \boldsymbol{x}\| = \sqrt{(\alpha\, \boldsymbol{x}) \cdot (\alpha\, \boldsymbol{x})} = \sqrt{\alpha^2\, \boldsymbol{x} \cdot \boldsymbol{x}} = \sqrt{\alpha^2} \cdot \sqrt{\boldsymbol{x} \cdot \boldsymbol{x}} = |\alpha| \cdot \|\boldsymbol{x}\|.$

8.20. Definice. Nechť L je lineární prostor se skalárním součinem a $\boldsymbol{x} \in L$, $\boldsymbol{y} \in L$, $\boldsymbol{x} \ne \boldsymbol{o}$, $\boldsymbol{y} \ne \boldsymbol{o}$. Pak *úhel mezi vektory* $\boldsymbol{x}$ *a* $\boldsymbol{y}$ je takové číslo $\varphi \in \langle 0, 2\pi)$, pro které platí *Úhel dvou vektorů*

$$\cos\varphi = \frac{\boldsymbol{x} \cdot \boldsymbol{y}}{\|\boldsymbol{x}\| \cdot \|\boldsymbol{y}\|}. \tag{8.2}$$

8.21. Poznámka. Zabývejme se otázkou, zda každé dva nenulové vektory mají definován úhel mezi sebou. Především podle poznámky 8.18 platí, že $\|\boldsymbol{x}\| \ne 0$, $\|\boldsymbol{y}\| \ne 0$, protože $\boldsymbol{x} \ne \boldsymbol{o}$, $\boldsymbol{y} \ne \boldsymbol{o}$. Takže se ve zlomku z rovnosti (8.2) nedělí nulou.

Aby existovalo φ takové, že platí (8.2), musí platit

$$-1 \le \frac{\boldsymbol{x} \cdot \boldsymbol{y}}{\|\boldsymbol{x}\| \cdot \|\boldsymbol{y}\|} \le 1.$$

Tento požadavek zaručuje následující věta.

8.22. Věta (Schwartzova nerovnost). Nechť L je lineární prostor se skalárním součinem a $\boldsymbol{x} \in L$, $\boldsymbol{y} \in L$. Pak platí:

$$|\boldsymbol{x} \cdot \boldsymbol{y}| \le \|\boldsymbol{x}\| \cdot \|\boldsymbol{y}\|. \tag{8.3}$$

Důkaz. Nechť $\alpha \in \mathbf{R}$. Násobme sám se sebou vektor $\boldsymbol{x} - \alpha\,\boldsymbol{y}$. Podle vlastnosti (4) definice 8.2 je

$$0 \le (\boldsymbol{x} - \alpha\,\boldsymbol{y}) \cdot (\boldsymbol{x} - \alpha\,\boldsymbol{y}) = \boldsymbol{x} \cdot \boldsymbol{x} - \alpha \cdot 2(\boldsymbol{x} \cdot \boldsymbol{y}) + \alpha^2 \cdot (\boldsymbol{y} \cdot \boldsymbol{y}).$$

V úpravách jsme použili vlastnosti (2) a (3) definice 8.2. Označme $A = \boldsymbol{y} \cdot \boldsymbol{y} = \|\boldsymbol{y}\|^2$, $B = -2(\boldsymbol{x} \cdot \boldsymbol{y})$, $C = \boldsymbol{x} \cdot \boldsymbol{x} = \|\boldsymbol{x}\|^2$. Dostáváme

$$0 \le A\,\alpha^2 + B\,\alpha + C.$$

Tato nerovnost musí platit pro všechna $\alpha \in \mathbf{R}$. Diskriminant této kvadratické nerovnice tedy nesmí být kladný. Z toho nám vyplývá podmínka pro čísla A, B, C:

$$B^2 - 4AC \le 0, \quad \text{tj.} \quad B^2 \le 4AC, \quad \text{tj.} \quad \big(-2(\boldsymbol{x} \cdot \boldsymbol{y})\big)^2 \le 4\,\|\boldsymbol{x}\|^2\|\boldsymbol{y}\|^2,$$
$$\text{tj.} \quad (-2)^2\,(\boldsymbol{x} \cdot \boldsymbol{y})^2 \le 4\,\|\boldsymbol{x}\|^2\|\boldsymbol{y}\|^2, \quad \text{tj.} \quad \sqrt{(\boldsymbol{x} \cdot \boldsymbol{y})^2} \le \sqrt{\|\boldsymbol{x}\|^2}\sqrt{\|\boldsymbol{y}\|^2} \quad \text{tj.} \quad |\boldsymbol{x} \cdot \boldsymbol{y}| \le \|\boldsymbol{x}\| \cdot \|\boldsymbol{y}\|.$$

8.23. Definice. Nechť L je lineární prostor se skalárním součinem. *Vzdálenost vektoru $\boldsymbol{x}$ od vektoru $\boldsymbol{y}$* definujeme jako $\|\boldsymbol{y} - \boldsymbol{x}\|$. Podle věty 8.19 je $\|\boldsymbol{y} - \boldsymbol{x}\| = \|\boldsymbol{x} - \boldsymbol{y}\|$, takže často mluvíme o *vzdálenosti dvou vektorů $\boldsymbol{x}$ a $\boldsymbol{y}$* (bez závislosti na jejich pořadí). *Vzdálenost vektorů*

8.24. Věta (trojúhelníková nerovnost). Pro velikosti vektorů platí

$$\|\boldsymbol{x} + \boldsymbol{y}\| \le \|\boldsymbol{x}\| + \|\boldsymbol{y}\|. \tag{8.4}$$

Důkaz. $\|\boldsymbol{x} + \boldsymbol{y}\|^2 = (\boldsymbol{x} + \boldsymbol{y}) \cdot (\boldsymbol{x} + \boldsymbol{y}) = \boldsymbol{x}\,\boldsymbol{x} + 2\,\boldsymbol{x}\,\boldsymbol{y} + \boldsymbol{y}\,\boldsymbol{y} \le \|\boldsymbol{x}\|^2 + 2\,\|\boldsymbol{x}\| \cdot \|\boldsymbol{y}\| + \|\boldsymbol{y}\|^2 = \big(\|\boldsymbol{x}\| + \|\boldsymbol{y}\|\big)^2$. Ve výpočtu jsme použili Schwartzovu nerovnost 8.22. Po odmocnění dostáváme dokazovanou nerovnost.

8.25. Poznámka. Vysvětlíme si, proč se dokázaná nerovnost nazývá trojúhelníková. Tu někteří čtenáři znají geometricky formulovanou třeba takto: součet délek dvou stran v trojúhelníku je vždy větší než délka strany třetí. Nechť vektory $\boldsymbol{a}$, $\boldsymbol{b}$ a $\boldsymbol{c}$ jsou prvky lineárního prostoru se skalárním součinem a představme si je jako vrcholy pomyslného trojúhelníka. Velikost stran je totéž jako vzdálenost odpovídajících vektorů. Geometrické tvrzení o velikostech stran trojúhelníka tedy můžeme pomocí definice 8.23 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 (8.4).

8.26. Příklad. Uvažujme lineární prostor $\mathbf{R}^4$ se standardním skalárním součinem (8.1). Ukážeme, jak vypadá velikost vektoru $(1, 2, 3, 4)$ a jaký je úhel mezi vektory $(1, 2, 3, 4)$ a $(1, 0, 0, 2)$.

Podle definice 8.17 a podle (8.1) je

$$\big\|(1, 2, 3, 4)\big\| = \sqrt{(1, 2, 3, 4) \cdot (1, 2, 3, 4)} = \sqrt{1^2 + 2^2 + 3^2 + 4^2} = \sqrt{30}.$$

Podle definice 8.20 platí pro úhel φ následující rovnost:

$$\cos\varphi = \frac{(1, 2, 3, 4) \cdot (1, 0, 0, 2)}{\big\|(1, 2, 3, 4)\big\| \cdot \big\|(1, 0, 0, 2)\big\|} = \frac{1 + 0 + 0 + 4 \cdot 2}{\sqrt{30} \cdot \sqrt{1 + 4}} = \frac{9}{\sqrt{150}}, \quad \text{tj.} \quad \varphi = \arccos\frac{9}{\sqrt{150}}.$$

8.27. Příklad. Nechť L je lineární prostor spojitých funkcí definovaných na konečném uzavřeném intervalu $D \subseteq \mathbf{R}$. Ukážeme, že předpis

$$f \cdot g = \int_D f(x)\,g(x)\,\mathrm{d}x$$

definuje skalární součin na lineárním prostoru L. Ověříme vlastnosti (1) až (4). Nechť $f \in L$, $g \in L$, $h \in L$ a $\alpha \in \mathbf{R}$. Pak platí

$$
\begin{aligned}
&(1)\quad f \cdot g = \int_D f(x)\, g(x)\, \mathrm{d}x = \int_D g(x)\, f(x)\, \mathrm{d}x = g \cdot f,\\
&(2)\quad (f+g)\cdot h = \int_D \big(f(x)+g(x)\big)\, h(x)\, \mathrm{d}x = \int_D \big(f(x)\, h(x) + g(x)\, h(x)\big)\, \mathrm{d}x =\\
&\qquad\qquad = \int_D f(x)\, h(x)\, \mathrm{d}x + \int_D g(x)\, h(x)\, \mathrm{d}x = f\cdot h + g\cdot h,\\
&(3)\quad (\alpha f)\cdot g = \int_D \alpha f(x)\, g(x)\, \mathrm{d}x = \alpha \cdot \int_D f(x)\, g(x)\, \mathrm{d}x = \alpha\,(f\cdot g),\\
&(4)\quad f\cdot f = \int_D f^2(x)\, \mathrm{d}x \ge 0,\\
&\qquad\qquad \int_D f^2(x)\, \mathrm{d}x = 0 \quad \text{jen tehdy, když } f(x) = 0\ \forall x \in D, \text{ protože } f \text{ je spojitá.}
\end{aligned}
$$

Příklad ilustruje, že i na lineárních prostorech nekonečné dimenze jsme schopni definovat skalární součin. Z tohoto skalárního součinu odvozená *norma funkce* f $\|f\|$, „úhel φ mezi funkcemi f a g“ a „vzdálenost dvou funkcí f a g“ $\|f-g\|$ se počítá takto:

$$
\|f\| = \sqrt{\int_D f^2(x)\, \mathrm{d}x}, \quad \varphi = \arccos \frac{\int_D f(x) g(x)\, \mathrm{d}x}{\sqrt{\int_D f^2(x)\, \mathrm{d}x \int_D g^2(x)\, \mathrm{d}x}}, \quad \|f-g\| = \sqrt{\int_D \big(f(x)-g(x)\big)^2\, \mathrm{d}x}.
$$

8.28. Poznámka. Protože máme na lineárních prostorech se skalárním součinem definován úhel mezi nenulovými vektory, můžeme pro každé dva nenulové vektory rozhodnout, kdy jsou na sebe kolmé. Je to tehdy, když je $\cos\varphi = 0$, neboli $\boldsymbol{x}\cdot\boldsymbol{y} = 0$. Z toho vyplývá následující definice. *Kolmé vektory*

8.29. Definice. Nechť L je lineární prostor se skalárním součinem. Dva nenulové vektory $\boldsymbol{x} \in L$ a $\boldsymbol{y} \in L$ *jsou na sebe kolmé* (značíme $\boldsymbol{x} \perp \boldsymbol{y}$), pokud je $\boldsymbol{x}\cdot\boldsymbol{y} = 0$.

8.30. Příklad. (Pythagorova věta.) Nechť $\boldsymbol{x} \in L$, $\boldsymbol{y} \in L$ jsou nenulové vektory, které jsou na sebe kolmé. Pak platí

$$\|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2 = \|\boldsymbol{x}-\boldsymbol{y}\|^2.$$

Zdůvodnění je jednoduché: $\|\boldsymbol{x}-\boldsymbol{y}\|^2 = (\boldsymbol{x}-\boldsymbol{y})\cdot(\boldsymbol{x}-\boldsymbol{y}) = \boldsymbol{x}\cdot\boldsymbol{x} - 2\boldsymbol{x}\cdot\boldsymbol{y} + \boldsymbol{y}\cdot\boldsymbol{y} = \|\boldsymbol{x}\|^2 - 2\cdot 0 + \|\boldsymbol{y}\|^2$. Geometrická interpretace tohoto příkladu je následující. Trojúhleník s vrcholy $\boldsymbol{o}$, $\boldsymbol{x}$ a $\boldsymbol{y}$ je pravoúhlý s pravým úhlem při vrcholu $\boldsymbol{o}$. Čísla $\|\boldsymbol{x}\|$, $\|\boldsymbol{y}\|$ jsou velikosti odvěsen a $\|\boldsymbol{x}-\boldsymbol{y}\|$ je velikost přepony.

8.31. Definice. Nechť $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ je báze lineárního prostoru se skalárním součinem. Bázi B nazýváme *ortogonální*, pokud $\boldsymbol{b}_i \perp \boldsymbol{b}_j$ $\forall i \in \{1,2,\ldots,n\}$, $\forall j \in \{1,2,\ldots,n\}$, $i \ne j$. *Ortonormální báze*

Bázi B nazýváme *ortonormální*, pokud je ortogonální, a navíc $\|\boldsymbol{b}_i\| = 1$, $\forall i \in \{1,2,\ldots,n\}$.

8.32. Věta. Báze $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ je ortonormální právě tehdy, když

$$\boldsymbol{b}_i \cdot \boldsymbol{b}_j = \begin{cases} 0 \text{ pro } i \ne j, \\ 1 \text{ pro } i = j. \end{cases}$$

Důkaz. Báze B je ortonormální právě tehdy, když (podle definice 8.31) platí $\boldsymbol{b}_i\cdot\boldsymbol{b}_j = 1$ pro $i = j$ a navíc je ortogonální, tj. $\boldsymbol{b}_i \perp \boldsymbol{b}_j$ pro $i \ne j$. To podle definice 8.29 znamená, že $\boldsymbol{b}_i\cdot\boldsymbol{b}_j = 0$ pro $i \ne j$.

8.33. Věta. Nechť (B) je ortonormální uspořádaná báze lineárního prostoru L se skalárním součinem. Pak pro všechna $\boldsymbol{x} \in L$, $\boldsymbol{y} \in L$, $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)_{(B)}$, $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)_{(B)}$ lze skalární součin počítat ze souřadnic vektorů takto:

$$\boldsymbol{x}\cdot\boldsymbol{y} = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n.$$

Důkaz. Podle předpokladu je $\boldsymbol{x} = x_1\,\boldsymbol{b}_1 + x_2\,\boldsymbol{b}_2 + \cdots + x_n\,\boldsymbol{b}_n$, $\boldsymbol{y} = y_1\,\boldsymbol{b}_1 + y_2\,\boldsymbol{b}_2 + \cdots + y_n\,\boldsymbol{b}_n$. Počítejme $\boldsymbol{x}\cdot\boldsymbol{y}$:

$$\boldsymbol{x}\cdot\boldsymbol{y} = (x_1\,\boldsymbol{b}_1 + x_2\,\boldsymbol{b}_2 + \cdots + x_n\,\boldsymbol{b}_n)\cdot(y_1\,\boldsymbol{b}_1 + y_2\,\boldsymbol{b}_2 + \cdots + y_n\,\boldsymbol{b}_n) =$$
$$= x_1y_1\,\boldsymbol{b}_1\cdot\boldsymbol{b}_1 + x_1y_2\,\boldsymbol{b}_1\cdot\boldsymbol{b}_2 + \cdots + x_1y_n\,\boldsymbol{b}_1\cdot\boldsymbol{b}_n + x_2y_1\,\boldsymbol{b}_2\cdot\boldsymbol{b}_1 + x_2y_2\,\boldsymbol{b}_2\cdot\boldsymbol{b}_2 + \cdots + x_2y_n\,\boldsymbol{b}_2\cdot\boldsymbol{b}_n + \cdots + x_ny_n\,\boldsymbol{b}_n\cdot\boldsymbol{b}_n =$$
$$= x_1y_1\cdot 1 + x_1y_2\cdot 0 + \cdots + x_1y_n\cdot 0 + x_2y_1\cdot 0 + x_2y_2\cdot 1 + \cdots + x_2y_n\cdot 0 + \cdots + x_ny_n\cdot 1 = x_1y_1 + x_2y_2 + \cdots + x_ny_n.$$

V úpravách jsme využili větu 8.32 a toho, že báze B je ortonormální.

8.34. Příklad. Nechť $\mathbf{R}^n$ je lineární prostor se standardním skalárním součinem zavedeným v příkladu 8.7. 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.

8.35. Věta. Nechť $\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_n$ jsou nenulové vektory lineárního prostoru se skalárním součinem, které jsou na sebe navzájem kolmé, tj. $\boldsymbol{x}_i\cdot\boldsymbol{x}_j = 0$ pro $i \neq j$ a $\boldsymbol{x}_i\cdot\boldsymbol{x}_i > 0$. Pak jsou tyto vektory lineárně nezávislé.

Důkaz. Podle definice lineární nézávislosti stačí ověřit, že z rovnosti

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

nutně plyne, že všechna čísla čísla α_i jsou nulová. Vynásobíme-li obě strany uvedené rovnosti skalárně vektorem $\boldsymbol{x}_i$, dostáváme na levé straně součet nul s výjimkou jediného sčítance, protože vektor $\boldsymbol{x}_i$ je kolmý na všechny všechny ostatní vektory $\boldsymbol{x}_j$. Máme tedy

$$\alpha_i\,\boldsymbol{x}_i\cdot\boldsymbol{x}_i = \boldsymbol{o}\cdot\boldsymbol{x}_i = 0.$$

Protože $\boldsymbol{x}_i\cdot\boldsymbol{x}_i$ je nenulové číslo, musí být $\alpha_i = 0$. Tuto operaci můžeme provést pro každý index $i \in \{1,2,\ldots,n\}$, takže všechna čísla čísla α_i jsou nutně nulová.

8.36. Věta. Nechť $(B) = (\boldsymbol{b}_1,\boldsymbol{b}_2,\ldots,\boldsymbol{b}_n)$ je ortonormální báze lineárního prostoru se skalárním součinem. Pak pro souřadnice libovolného vektoru $\boldsymbol{x}$ platí

$$\boldsymbol{x} = (\boldsymbol{x}\cdot\boldsymbol{b}_1,\ \boldsymbol{x}\cdot\boldsymbol{b}_2,\ \ldots,\ \boldsymbol{x}\cdot\boldsymbol{b}_n)_{(B)}.$$

Důkaz. Označme $\boldsymbol{y} = (\boldsymbol{x}\cdot\boldsymbol{b}_1)\,\boldsymbol{b}_1 + (\boldsymbol{x}\cdot\boldsymbol{b}_2)\,\boldsymbol{b}_2 + \cdots + (\boldsymbol{x}\cdot\boldsymbol{b}_n)\,\boldsymbol{b}_n$. Podle definice souřadnic vzhledem k bázi máme dokázat, že $\boldsymbol{x} = \boldsymbol{y}$. Násobme vektor $\boldsymbol{y}$ vektorem $\boldsymbol{b}_i$:

$$\boldsymbol{y}\cdot\boldsymbol{b}_i = \big((\boldsymbol{x}\cdot\boldsymbol{b}_1)\,\boldsymbol{b}_1 + (\boldsymbol{x}\cdot\boldsymbol{b}_2)\,\boldsymbol{b}_2 + \cdots + (\boldsymbol{x}\cdot\boldsymbol{b}_n)\,\boldsymbol{b}_n\big)\cdot\boldsymbol{b}_i = (\boldsymbol{x}\cdot\boldsymbol{b}_i)\,\boldsymbol{b}_i\cdot\boldsymbol{b}_i = \boldsymbol{x}\cdot\boldsymbol{b}_i,$$

protože báze (B) je ortonormální. Máme tedy výsledek $\boldsymbol{x}\cdot\boldsymbol{b}_i = \boldsymbol{y}\cdot\boldsymbol{b}_i$ $\forall i \in \{1,2,\ldots,n\}$.

Vektor $\boldsymbol{x}-\boldsymbol{y}$ je kolmý na všechny prvky $\boldsymbol{b}_i$, protože z předchozího výpočtu plyne $(\boldsymbol{x}-\boldsymbol{y})\cdot\boldsymbol{b}_i = 0$. Pokud by $\boldsymbol{x} \neq \boldsymbol{y}$, pak podle věty 8.35 jsou vektory $\boldsymbol{b}_1,\boldsymbol{b}_2,\ldots,\boldsymbol{b}_n,\boldsymbol{x}-\boldsymbol{y}$ lineárně nezávislé, ale to je ve sporu s tím, že (B) je báze. Musí tedy být $\boldsymbol{x} = \boldsymbol{y}$.

8.37. Poznámka. Předchozí věta má názornou geometrickou interpretaci. Souřadnice $\boldsymbol{x}\cdot\boldsymbol{b}_i$ jsou vlastně kolmé průměty vektoru $\boldsymbol{x}$ na vektory báze $\boldsymbol{b}_i$. O těchto pojmech pohovoříme podrobněji v následující kapitole.

8.38. Věta. Nechť $(B) = (\boldsymbol{b}_1,\boldsymbol{b}_2,\ldots,\boldsymbol{b}_n)$ je ortonormální báze lineárního prostoru se skalárním součinem a $\boldsymbol{x} = (x_1,x_2,\ldots,x_n)_{(B)}$ je jeho libovolný vektor. Pak úhel φ_i mezi vektorem $\boldsymbol{x}$ a vektorem $\boldsymbol{b}_i$ lze počítat podle vzorce

$$\cos\varphi_i = \frac{x_i}{\|\boldsymbol{x}\|}\,.$$

Důkaz. Podle definice 8.20 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 8.36, podle které je $x_i = \boldsymbol{x}\cdot\boldsymbol{b}_i$.

8.39. Poznámka. Protože je $\|\boldsymbol{x}\|^2/\|\boldsymbol{x}\|^2 = 1$ a dále je $\|\boldsymbol{x}\|^2 = x_1^2 + x_2^2 + \cdots + x_n^2$, plyne z věty 8.38 zajímavý důsledek:

$$\cos^2\varphi_1 + \cos^2\varphi_2 + \cdots + \cos^2\varphi_n = 1,$$

kde φ_i jsou úhly mezi vektorem $\boldsymbol{x}$ a vektory ortonormální báze.

Ortogonalizační proces

8.40. Poznámka. Je přirozené se ptát, zda každý lineární prostor (aspoň konečné dimenze) má ortonormální bázi. Věta 2.51 ukazuje, že každý lineární prostor má bázi. Následující věta ukazuje, že každá konečná báze se dá v jistém smyslu pozměnit tak, aby se z ní stala ortonormální báze.

8.41. Věta (Schmidtův ortogonalizační proces). Nechť $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ je báze lineárního prostoru L se skalárním součinem. Pak existuje ortonormální báze $\{\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n\}$ taková, že

$$\langle \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k\rangle = \langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k\rangle, \qquad \forall k \in \{1, 2, \ldots, n\}.$$

Důkaz. Nejprve vysvětlíme ideu důkazu, která je v tomto případě asi důležitější než podrobné počítání. Vektor $\boldsymbol{c}_1$ volíme stejný jako $\boldsymbol{b}_1$ jen s tím rozdílem, že jej „normalizujeme“. To znamená, že jej násobíme vhodnou konstantou, aby $\|\boldsymbol{c}_1\| = 1$.

Představme si dále, že už jsme našli $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$ takové, že $\langle \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k\rangle = \langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k\rangle$, a přitom vektory $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$ jsou na sebe vzájemně kolmé a mají jednotkovou velikost. Vektor $\boldsymbol{b}_{k+1}$ nyní „ortogonalizujeme“, tj. upravíme tak, aby byl kolmý na všechny vektory z $\langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k\rangle$. Ukážeme později, že k tomu účelu stačí od vektoru $\boldsymbol{b}_{k+1}$ odečíst určitou lineární kombinaci vektorů $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$. Takto upravený vektor dále „normalizujeme“, tj. vynásobíme vhodnou konstantou, aby $\|\boldsymbol{c}_{k+1}\| = 1$. Tím se jeho kolmost vůči ostatním vektorům z $\langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k\rangle$ nepokazí. Protože vektor $\boldsymbol{c}_{k+1}$ vznikl jako lineární kombinace vektorů $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k, \boldsymbol{b}_{k+1}$, je

$$\langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k, \boldsymbol{c}_{k+1}\rangle = \langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k, \boldsymbol{b}_{k+1}\rangle = \langle \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_{k+1}\rangle.$$

Tím jsme rozšířili naši novou postupně budovanou ortonormální bázi o další vektor. Opakovaným použitím tohoto postupu dostáváme hledanou ortonormální bázi $\{\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n\}$.

Nyní stačí jen podrobněji ukázat, jak se vektor „normalizuje“ a „ortogonalizuje“. Normalizaci libovolného vektoru $\boldsymbol{x}$ provedeme tak, že položíme $\boldsymbol{x}' = (1/\|\boldsymbol{x}\|)\cdot\boldsymbol{x}$. Skutečně je:

$$\|\boldsymbol{x}'\|^2 = \boldsymbol{x}'\cdot\boldsymbol{x}' = \frac{1}{\|\boldsymbol{x}\|}\,\boldsymbol{x}\cdot\frac{1}{\|\boldsymbol{x}\|}\,\boldsymbol{x} = \frac{1}{\|\boldsymbol{x}\|^2}\,\boldsymbol{x}\,\boldsymbol{x} = \frac{1}{\|\boldsymbol{x}\|^2}\,\|\boldsymbol{x}\|^2 = 1.$$

Nechť $\boldsymbol{b}_{k+1} \notin \langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k\rangle$ a nechť vektory $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$ jsou na sebe navzájem kolmé a mají jednotkovou velikost. Vektor $\boldsymbol{b}_{k+1}$ „ortogonalizujeme“ tak, že položíme

$$\boldsymbol{b}'_{k+1} = \boldsymbol{b}_{k+1} - \sum_{i=1}^{k}(\boldsymbol{b}_{k+1}\cdot\boldsymbol{c}_i)\,\boldsymbol{c}_i.$$

Nově vytvořený vektor $\boldsymbol{b}'_{k+1}$ je kolmý na všechny vektory $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$, protože:

$$\boldsymbol{b}'_{k+1}\cdot\boldsymbol{c}_j = \left(\boldsymbol{b}_{k+1} - \sum_{i=1}^{k}(\boldsymbol{b}_{k+1}\cdot\boldsymbol{c}_i)\,\boldsymbol{c}_i\right)\cdot\boldsymbol{c}_j = \boldsymbol{b}_{k+1}\cdot\boldsymbol{c}_j - \sum_{i=1}^{k}(\boldsymbol{b}_{k+1}\cdot\boldsymbol{c}_i)\,(\boldsymbol{c}_i\cdot\boldsymbol{c}_j) = \boldsymbol{b}_{k+1}\cdot\boldsymbol{c}_j - \boldsymbol{b}_{k+1}\cdot\boldsymbol{c}_j = 0.$$

V uvedeném součtu jsou ostatní sčítanci nuloví, protože vektory $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$ jsou podle předpokladu na sebe navzájem kolmé.

9. Aplikace lineární algebry v geometrii

9.1. Poznámka. Budeme pracovat s bodovým euklidovským prostorem. Bohužel nemáme zde místo na podrobné definování základních pojmů tohoto prostoru. Vycházíme tedy z toho, že čtenář intuitivně tuší, co to je bod, úsečku si představí jako nejkratší spojnici mezi dvěma body, nebo jako množinu bodů, která tuto spojnici vyplňuje. Jiné množiny bodů vytvářejí přímky nebo roviny. Všechny tyto množiny bodů jsou podmnožinami třírozměrného bodového euklidovského prostoru, označovaného obvykle $\mathbf{E}_3$. Jeho „třírozměrnost“ vyplývá z toho, že jsme schopni v tomto prostoru sestrojit maximálně tři na sebe navzájem kolmé přímky. Rovněž to souvisí s tím, že lineární prostory orientovaných úseček v $\mathbf{E}_3$ mají dimenzi rovnu třem. V bodovém prostoru $\mathbf{E}_3$ umíme měřit vzdálenost mezi libovolnými dvěma body a úhel mezi dvěma úsečkami, které mají společný jeden krajní bod. Předpokládáme tedy, že jsme vybaveni nějakým měřítkem a úhloměrem. Stupnice na našem měřítku vychází z nějaké jednotky vzdálenosti (metr, stopa aj.) a nebudeme tuto jednotku při popisování geometrických vlastností dále zmiňovat. *Euklidovský prostor*

9.2. Příklad. V příkladech 1.24 a 2.24 jsme zavedli lineární prostor vázaných vektorů U_O tak, že jsme zvolili jeden bod prostoru $\mathbf{E}_3$ a označili jej O. Na množině všech orientovaných úseček začínajících v bodě O jsme definovali sčítání (doplněním na rovnoběžník) a násobení konstantou (násobením velikosti úsečky). V příkladě 1.24 jsme ukázali, že množina takových úseček tvoří lineární prostor podle obecné definice lineárního prostoru a v příkladě 2.24 jsme naznačili, jak souvisí pojmy lineární závislost a nezávislost vektorů s geometrickými vlastnostmi lineárního prostoru U_O.

Zopakujeme nyní hlavní výsledky těchto příkladů a přidáme další poznatky. Nulový vektor $\boldsymbol{o} \in U_O$ je úsečka s nulovou velikostí, tj. koncový bod splývá s počátečním bodem. Jeden vektor $\boldsymbol{u} \in U_O$ je lineárně nezávislý právě tehdy, když je nenulový. Dva vektory $\{\boldsymbol{u}, \boldsymbol{v}\} \subset U_O$ jsou lineárně nezávislé právě tehdy, když neleží ve společné přímce. Tři vektory $\{\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}\} \subset U_O$ jsou lineárně nezávislé právě tehdy, když neleží ve společné rovině. Čtyři vektory z U_O jsou vždy lineárně závislé. Z toho plyne, že $\dim U_O = 3$ a bázi U_O tvoří libovolné tři vektory, které neleží ve společné rovině.

Je-li $\boldsymbol{u} \in U_O$ nenulový, pak $\langle \boldsymbol{u} \rangle$ je množina vektorů, jejichž koncové body vyplňují přímku procházející bodem O. Jsou-li $\{\boldsymbol{u}, \boldsymbol{v}\} \subset U_O$ lineárně nezávislé, pak $\langle \boldsymbol{u}, \boldsymbol{v} \rangle$ je množina vektorů, jejichž koncové body vyplňují rovinu procházející bodem O. Jsou-li konečně tři vektory $\{\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}\} \subset U_O$ lineárně nezávislé, pak koncové body vektorů z $\langle \boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \rangle$ vyplňují celý prostor $\mathbf{E}_3$.

Je-li $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3\} \subset U_O$ lineárně nezávislá množina, pak tvoří bázi U_O a pro každý vektor $\boldsymbol{u} \in U_O$ existuje právě jedna lineární kombinace vektorů $\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3$, která je rovna vektoru $\boldsymbol{u}$. Koeficienty této lineární kombinace jsou podle definice 6.10 souřadnicemi vektoru $\boldsymbol{u}$ vzhledem k uspořádané bázi (B). Tyto souřadnice tvoří uspořádanou trojici reálných čísel a zobrazení, které každému vektoru $\boldsymbol{u} \in U_O$ přiřadí uspořádanou trojici jeho souřadnic z $\mathbf{R}^3$ je podle příkladu 7.25 izomorfismus. Toto zobrazení přenáší pojmy lineární závislost, podprostor a lineární obal z „geometrického“ lineárního prostoru U_O na „numerický“ lineární prostor $\mathbf{R}^3$. Jinými slovy, místo abychom zjišťovali tyto pojmy na lineárním prostoru U_O, kde sčítání je definováno doplňováním na rovnoběžník (potřebujeme dvě pravítka resp. kružítko na konstruování rovnoběžníků), budeme je ověřovat jen numericky v $\mathbf{R}^3$ (vystačíme si se sčítáním a násobením reálných čísel). To je základním principem tzv. *analytické geometrie.* Tuto teorii rozpracoval v 17. století francouzský matematik René Descartes. Po něm se nazývá souřadnicový systém kartézský. *Souřadnice orientovaných úseček*

9.3. Příklad. Na lineárním prostoru U_O nyní definujeme skalární součin. Nechť $\boldsymbol{u}$ a $\boldsymbol{v}$ jsou dvě orientované úsečky začínající v bodě O. Pokud je aspoň jedna z nich nulová, definujeme skalární součin $\boldsymbol{u} \cdot \boldsymbol{v} = 0$. Jsou-li obě úsečky nenulové, pak existuje rovina ϱ, ve které leží společně obě úsečky. Přiložíme v této rovině úhloměr k daným úsečkám a změříme úhel φ mezi těmito úsečkami. Skalární součin pak definujeme vzorcem *Skalární součin orientovaných úseček*

$$\boldsymbol{u} \cdot \boldsymbol{v} = \|\boldsymbol{u}\| \, \|\boldsymbol{v}\| \, \cos\varphi, \tag{9.1}$$

kde $\|\boldsymbol{u}\|$ a $\|\boldsymbol{v}\|$ jsou velikosti těchto úseček zjištěné měřítkem.

Ukážeme, že uvedený vzorec definuje skalární součin v souladu s obecnou definicí 8.2, tj. že platí vlastnosti (1) až (4).

(1) $\boldsymbol{u} \cdot \boldsymbol{v} = \|\boldsymbol{u}\| \, \|\boldsymbol{v}\| \cos\varphi = \|\boldsymbol{v}\| \, \|\boldsymbol{u}\| \cos\varphi = \boldsymbol{v} \cdot \boldsymbol{u}$,

(2) $(\boldsymbol{u} + \boldsymbol{v}) \cdot \boldsymbol{w} \overset{?}{=} \boldsymbol{u} \cdot \boldsymbol{w} + \boldsymbol{v} \cdot \boldsymbol{w}$ (vysvětlíme později),

(3) $(\alpha\, \boldsymbol{u}) \cdot \boldsymbol{v} = \|\alpha\, \boldsymbol{u}\| \, \|\boldsymbol{v}\| \cos\varphi = \begin{cases} \alpha\|\boldsymbol{u}\| \, \|\boldsymbol{v}\| \cos\varphi = \alpha\,(\boldsymbol{u} \cdot \boldsymbol{v}), & \text{pro } \alpha \geq 0, \\ -\alpha\|\boldsymbol{u}\| \, \|\boldsymbol{v}\| \cos(\varphi + \pi) = \alpha\|\boldsymbol{u}\| \, \|\boldsymbol{v}\| \cos\varphi = \alpha\,(\boldsymbol{u} \cdot \boldsymbol{v}), & \text{pro } \alpha < 0, \end{cases}$

(4) $\boldsymbol{u} \cdot \boldsymbol{u} = \|\boldsymbol{u}\|^2 \cos 0 = \|\boldsymbol{u}\|^2 \geq 0$.

Předpokládejme ještě $\boldsymbol{u} \cdot \boldsymbol{u} = \|\boldsymbol{u}\|^2 = 0$. Z toho plyne, že velikost úsečky $\boldsymbol{u}$ je nulová, takže nutně musí být $\boldsymbol{u} = \boldsymbol{o}$.

Zbývá nám dokázat vlastnost (2). Jsou-li některé z úseček nulové, je tvrzení (2) okamžitě splněno. Nechť jsou tedy všechny tři úsečky nenulové. Nechť dále φ_1 je úhel mezi $\boldsymbol{u}$ a $\boldsymbol{w}$. Označme $p_1 = \|\boldsymbol{u}\| \cos\varphi_1$ velikost kolmého průmětu úsečky $\boldsymbol{u}$ na úsečku $\boldsymbol{w}$. Ze vzorce (9.1) vidíme, že $p_1 = \boldsymbol{u} \cdot \boldsymbol{w}/\|\boldsymbol{w}\|$. Označme ještě p_2 velikost kolmého průmětu úsečky $\boldsymbol{v}$ na úsečku $\boldsymbol{w}$ a konečně p_0 velikost kolmého průmětu součtu $\boldsymbol{u}+\boldsymbol{v}$ na úsečku $\boldsymbol{w}$. Z geometrických vlastností rovnoběžníků a průmětů plyne, že $p_0 = p_1 + p_2$ (udělejte si náčrtek). Protože platí

$$p_1 = \frac{\boldsymbol{u} \cdot \boldsymbol{w}}{\|\boldsymbol{w}\|}, \quad p_2 = \frac{\boldsymbol{v} \cdot \boldsymbol{w}}{\|\boldsymbol{w}\|}, \quad p_0 = \frac{(\boldsymbol{u}+\boldsymbol{v}) \cdot \boldsymbol{w}}{\|\boldsymbol{w}\|},$$

je po vynásobení rovnosti $p_0 = p_1 + p_2$ číslem $\|\boldsymbol{w}\|$ požadovaná rovnost (2) dokázána.

9.4. Poznámka. Při ověřování vlastnosti (4) jsme mimochodem zjistili, že velikost úsečky odvozená ze skalárního součinu (definice 8.17) je rovna velikosti úsečky zjištěné měřítkem. Úhel mezi úsečkami podle definice 8.20 je také roven skutečnému úhlu mezi úsečkami. To plyne přímo ze vzorce (9.1).

9.5. Poznámka. K definování skalárního součinu na lineárním prostoru orientovaných úšeček jsme v předchozím příkladu použili kromě měřítka ještě úhloměr a nějaký stroj, který nám vyhodnotí funkci kosinus. Ukážeme, že lze modifikovat definici tak, že místo úhloměru a stroje na kosinus si vystačíme jen s pravítkem s ryskou (na sestrojování kolmic).

Nechť $\boldsymbol{u}$ a $\boldsymbol{v}$ jsou nenulové orientované úsečky začínající ve společném bodě O. Nechť p je přímka, která obsahuje úsečku $\boldsymbol{v}$. Pomocí pravítka s ryskou sestrojíme kolmici na přímku p, která prochází koncovým bodem úsečky $\boldsymbol{u}$. Průsečík přímky p a sestrojené kolmice označme P. Nyní definujeme

$$\boldsymbol{u} \cdot \boldsymbol{v} = \pm\|\boldsymbol{v}\| \cdot \text{velikost úsečky } OP,$$

kde místo znaku „$\pm$" použijeme znaménko „$+$", je-li úsečka OP shodně orientovaná s úsečkou $\boldsymbol{v}$, a použijeme znaménko „$-$", jsou-li tyto úsečky opačně orientované.

Uvědomíme si, že úsečka OP je kolmým průmětem úsečky $\boldsymbol{u}$ na přímku p, velikost tohoto průmětu je podle kosinové věty rovna (až na znaménko) číslu $\|\boldsymbol{u}\| \cos\varphi$, kde φ je úhel mezi úsečkami $\boldsymbol{u}$ a $\boldsymbol{v}$. Vidíme tedy, že je definice skalárního součinu shodná s definicí podle vzorce (9.1).

Kolmý průmět vektoru na vektor

Kolmý průmět vektoru $\boldsymbol{u}$ na nenulový vektor $\boldsymbol{v}$ je názorná geometrická aplikace skalárního součinu a má obecnou platnost i v lineárních prostorech s větší dimenzí. Stojí za to tento pojem formálně definovat pro libovolný lineární prostor se skalárním součinem:

9.6. Definice. Nechť L je lineární prostor se skalárním součinem, $\boldsymbol{u} \in L, \boldsymbol{v} \in L, \boldsymbol{v} \neq \boldsymbol{o}$. Pak vektor

$$\frac{\boldsymbol{u} \cdot \boldsymbol{v}}{\|\boldsymbol{v}\|^2}\, \boldsymbol{v}$$

nazýváme *kolmý průmět vektoru* $\boldsymbol{u}$ *na vektor* $\boldsymbol{v}$.

Číslo $(\boldsymbol{u} \cdot \boldsymbol{v}) \,/\, \|\boldsymbol{v}\|$ je velikost kolmého průmětu vektoru $\boldsymbol{u}$ na vektor $\boldsymbol{v}$ „až na znaménko". Toto číslo je záporné právě tehdy, když kolmý průmět na vektor $\boldsymbol{v}$ má opačný směr než vektor $\boldsymbol{v}$.

Ortonormální báze v U_O

9.7. Příklad. Nechť U_O je lineární prostor se skalárním součinem z příkladu 9.3. Sestrojíme dvě orientované úsečky začínající v bodě O s velikostí 1, které jsou na sebe kolmé (ověříme úhloměrem). Tyto dvě úsečky leží v jednoznačně určené rovině ϱ. Sestrojíme třetí úsečku velikosti 1, která začíná v bodě O a je kolmá na rovinu ϱ. Tyto tři úsečky označíme $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$. Je zřejmé, že $B = \{\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}$ je ortonormální bází lineárního prostoru U_O.

9.8. Poznámka. Souřadnice vektoru $\boldsymbol{u} \in U_O$ vzhledem k ortonormální bázi $B = \{\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}$ jsou podle věty 8.36 a definice 9.6 velikostmi (až na znaménko) kolmých průmětů vektoru $\boldsymbol{u}$ na vektory $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$. To nám umožňuje velmi snadno najít souřadnice geometrickými prostředky a dále se souřadnicemi (uspořádanými trojicemi v $\mathbf{R}^3$) pracovat numericky.

9.9. Příklad. Nechť $B = \{\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}$ je báze z příkladu 9.7. Uspořádejme tuto bázi, tj. záleží nám na pořadí prvků $\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$. Vidíme, že jakákoli jiná uspořádaná ortonormální báze vzniká současným otočením úseček $\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ kolem bodu O nebo současným otočením úseček $\boldsymbol{i}, \boldsymbol{j}, -\boldsymbol{k}$ kolem bodu O. Přechod mezi bází $(B) = \big(\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\big)$ a $(B') = \big(\boldsymbol{i}, \boldsymbol{j}, -\boldsymbol{k}\big)$ nelze realizovat současným otočením všech úseček.

Dá se ukázat, že pokud báze C vzniká z báze B otočením úseček kolem bodu O, má matice přechodu $\mathbf{A}_{(B,C)}$ kladný determinant. Dále matice přechodu od báze B k bázi B' vypadá takto

$$\mathbf{A}_{(B,B')} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Je tedy $\det \mathbf{A}_{(B,B')} = -1$. To nás vede k následující definici kladně orientované báze.

9.10. Definice. Nechť U_O je lineární prostor se skalárním součinem podle příkladu 9.3. Ortonormální uspořádanou bázi $(B) = \big(\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\big)$ nazýváme *kladně orientovanou*, pokud při vhodném umístění a natočení pozorovatele vzhledem k této bázi směřuje úsečka $\boldsymbol{i}$ směrem k pozorovateli, $\boldsymbol{j}$ vpravo od pozorovatele a $\boldsymbol{k}$ nahoru.

Kladně orientovaná báze

Mnemotechnickou pomůckou je tzv. *pravidlo pravé ruky.* Přiložíme-li pravou ruku k vektorům $\boldsymbol{i}$, $\boldsymbol{j}$ tak, aby prsty směřovaly od $\boldsymbol{i}$ k $\boldsymbol{j}$, potom palec naznačuje směr vektoru $\boldsymbol{k}$.

Všechny báze (C) (ne nutně ortonormální), které mají matici přechodu od (B) k (C) s kladným determinantem, nazýváme *kladně orientované báze.* Všechny báze (D), které mají matici přechodu od (B) k (D) se záporným determinantem, nazýváme *záporně orientované báze.*

9.11. Poznámka. Na lineárním prostoru U_O jsme rozdělili všechny báze do dvou skupin: kladně orientované báze a záporně orientované báze. Matice přechodu je podle věty 6.19 vždy regulární, takže je jednoznačně dáno, zda je báze kladně nebo záporně orientovaná (determinant matice přechodu je vždy nenulový).

Podle vět 6.27 a 4.35 také okamžitě vidíme, že matice přechodu mezi kladně orientovanými bázemi má vždy kladný determinant, matice přechodu mezi záporně orientovanými bázemi má také kladný determinant a matice přechodu od kladně orientované báze k záporně orientované bázi má záporný determinant stejně jako matice přechodu od záporně orientované báze ke kladně orientované bázi.

9.12. Poznámka. V libovolném lineárním prostoru konečné dimenze jsme schopni rozlišit dvě skupiny uspořádaných bází tak, že matice přechodu od báze z jedné skupiny k bázi v druhé skupině má záporný determinant a matice přechodu od báze k bázi uvnitř skupiny má kladný determinant. Nejedná se tedy jen o geometrickou vlastnost lineárního prostoru U_O. Je proto vhodné uvést následující obecnou definici:

9.13. Definice. *Orientovat* libovolný lineární prostor s konečnou dimenzí znamená prohlásit jednu jeho uspořádanou bázi (B) za výchozí kladně orientovanou. Uspořádaná báze (C) se nazývá *kladně orientovaná*, pokud matice přechodu od výchozí báze (B) k bázi (C) má kladný determinant. Uspořádaná báze (D) se nazývá *záporně orientovaná*, pokud matice přechodu od výchozí báze (B) k bázi (D) má záporný determinant.

9.14. Příklad. Orientaci lineárního prostoru U_O jsme provedli v definici 9.10.

9.15. Poznámka. Již dříve jsme mluvili o „orientovaných“ úsečkách. Ačkoli jsme použili stejné slovo, s orientací lineárního prostoru to příliš nesouvisí. Orientace úsečky znamená určení pořadí jejích krajních bodů, nebo (jinak řečeno) rozlišení mezi počátečním a konečným bodem úsečky.

9.16. Poznámka. V další části textu definujeme *vektorový součin*, což je operace, která dvěma vektorům přiřadí jako výsledek vektor (na rozdíl od skalárního součinu, který dvěma vektorům přiřadí číslo, neboli skalár). Vektorový součin definujeme prozatím na lineárním prostoru U_O orientovaných úseček, který již známe z příkladů 9.2, 9.3, 9.7 a 9.14.

Vektorový součin

9.17. Definice. Nechť U_O je lineární prostor orientovaných úseček. *Vektorový součin* je zobrazení (označujeme jej křížkem) $\times : U_O \times U_O \to U_O$, které splňuje následující vlastnosti.

(A) Jsou-li vektory $\{\boldsymbol{u}, \boldsymbol{v}\} \subset U_O$ lineárně závislé, definujeme $\boldsymbol{u} \times \boldsymbol{v} = \boldsymbol{o}$ (nulový vektor).

(B) Jsou-li vektory $\{\boldsymbol{u}, \boldsymbol{v}\} \subset U_O$ lineárně nezávislé, pak je vektor $\boldsymbol{u} \times \boldsymbol{v}$ jednoznačně určen následujícími třemi vlastnostmi:

(1) $(\boldsymbol{u} \times \boldsymbol{v}) \perp \boldsymbol{u}$, $(\boldsymbol{u} \times \boldsymbol{v}) \perp \boldsymbol{v}$,

(2) $\|\boldsymbol{u} \times \boldsymbol{v}\| = \|\boldsymbol{u}\|\,\|\boldsymbol{v}\| \sin\varphi$, kde φ je úhel mezi vektory $\boldsymbol{u}$ a $\boldsymbol{v}$.

(3) Uspořádaná báze $(\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{u} \times \boldsymbol{v})$ je kladně orientovaná.

9.18. Poznámka. Vidíme, že skutečně vlastnosti (1) až (3) určují vektorový součin jednoznačně. První vlastnost udává, že výsledek bude kolmý na rovinu určenou $\langle \boldsymbol{u}, \boldsymbol{v}\rangle$, druhá vlastnost určuje velikost výsledného vektoru a třetí vlastnost orientaci (zda výsledný vektor bude orientován vzhledem k rovině určené $\langle \boldsymbol{u}, \boldsymbol{v}\rangle$ „nahoru“ nebo „dolu“.

9.19. Příklad. Nechť $(B) = (\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k})$ je ortonormální kladně orientovaná uspořádaná báze lineárního prostoru U_O. Pak podle definice je

$$\boldsymbol{i} \times \boldsymbol{i} = \boldsymbol{j} \times \boldsymbol{j} = \boldsymbol{k} \times \boldsymbol{k} = \boldsymbol{o},$$
$$\boldsymbol{i} \times \boldsymbol{j} = \boldsymbol{k}, \quad \boldsymbol{j} \times \boldsymbol{i} = -\boldsymbol{k}, \quad \boldsymbol{i} \times \boldsymbol{k} = -\boldsymbol{j}, \quad \boldsymbol{k} \times \boldsymbol{i} = \boldsymbol{j}, \quad \boldsymbol{j} \times \boldsymbol{k} = \boldsymbol{i}, \quad \boldsymbol{k} \times \boldsymbol{j} = -\boldsymbol{i}.$$

9.20. Věta (souřadnice vektorového součinu). Nechť $(B) = (\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k})$ je ortonormální kladně orientovaná uspořádaná báze lineárního prostoru U_O, $\boldsymbol{u} = (u_1, u_2, u_3)_{(B)}$, $\boldsymbol{v} = (v_1, v_2, v_3)_{(B)}$. Pak platí:

$$\boldsymbol{u} \times \boldsymbol{v} = \left(\begin{vmatrix} u_2 & u_3 \\ v_2 & v_3 \end{vmatrix}, - \begin{vmatrix} u_1 & u_3 \\ v_1 & v_3 \end{vmatrix}, \begin{vmatrix} u_1 & u_2 \\ v_1 & v_2 \end{vmatrix} \right)_{(B)}. \tag{9.2}$$

Důkaz. Pokud jsou vektory $\boldsymbol{u}, \boldsymbol{v}$ lineárně závislé, pak všechny determinanty ve vzorci (9.2) jsou nulové a výsledný vektor $\boldsymbol{u} \times \boldsymbol{v}$ má nulové souřadnice, takže je v souladu s definicí nulový. Zbývá tedy ověřit vlastnosti (1) až (3) z definice vektorového součinu pro případ, že vektory $\boldsymbol{u}, \boldsymbol{v}$ jsou lineárně nezávislé.

Ad (1). Ověříme $(\boldsymbol{u} \times \boldsymbol{v}) \perp \boldsymbol{u}$. Dva vektory jsou kolmé, pokud jejich skalární součin je nulový. Skalární součin můžeme počítat ze souřadnic podle věty 8.33:

$$\begin{vmatrix} u_2 & u_3 \\ v_2 & v_3 \end{vmatrix} u_1 - \begin{vmatrix} u_1 & u_3 \\ v_1 & v_3 \end{vmatrix} u_2 + \begin{vmatrix} u_1 & u_2 \\ v_1 & v_2 \end{vmatrix} u_3 = \begin{vmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \\ u_1 & u_2 & u_3 \end{vmatrix} = 0.$$

Při úpravách jsme využili rozvoje determinantu podle třetího řádku a dále toho, že determinant je roven nule, pokud se v něm dva řádky opakují. Podobně by to dopadlo při ověřování $(\boldsymbol{u} \times \boldsymbol{v}) \perp \boldsymbol{v}$.

Ad (2).

$$\|\boldsymbol{u} \times \boldsymbol{v}\|^2 = \begin{vmatrix} u_2 & u_3 \\ v_2 & v_3 \end{vmatrix}^2 + \begin{vmatrix} u_1 & u_3 \\ v_1 & v_3 \end{vmatrix}^2 + \begin{vmatrix} u_1 & u_2 \\ v_1 & v_2 \end{vmatrix}^2 = \textit{poněkud pracnější výpočet je zde vynechán} =$$
$$= (u_1^2 + u_2^2 + u_3^2)\,(v_1^2 + v_2^2 + v_3^2) - (u_1 v_1 + u_2 v_2 + u_3 v_3)^2 = \|\boldsymbol{u}\|^2\,\|\boldsymbol{v}\|^2 - (\boldsymbol{u} \cdot \boldsymbol{v})^2 =$$
$$= \|\boldsymbol{u}\|^2\,\|\boldsymbol{v}\|^2 - \|\boldsymbol{u}\|^2\,\|\boldsymbol{v}\|^2 \cos^2\varphi = \|\boldsymbol{u}\|^2\,\|\boldsymbol{v}\|^2 (1 - \cos^2\varphi) = \|\boldsymbol{u}\|^2\,\|\boldsymbol{v}\|^2 \sin^2\varphi.$$

Po odmocnění vychází požadovaná vlastnost.

Ad (3). Především velikost vektoru $\boldsymbol{u} \times \boldsymbol{v}$ je pro lineárně nezávislé vektory $\boldsymbol{u}, \boldsymbol{v}$ nenulová a tento vektor je kolmý na oba vektory $\boldsymbol{u}, \boldsymbol{v}$. Množina $\{\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{u} \times \boldsymbol{v}\}$ tedy tvoří bázi lineárního prostoru U_O. Matice

$$\mathbf{A} = \begin{pmatrix} u_1 & v_1 & \begin{vmatrix} u_2 & u_3 \\ v_2 & v_3 \end{vmatrix} \\ u_2 & v_2 & -\begin{vmatrix} u_1 & u_3 \\ v_1 & v_3 \end{vmatrix} \\ u_3 & v_3 & \begin{vmatrix} u_1 & u_2 \\ v_1 & v_2 \end{vmatrix} \end{pmatrix}$$

je maticí přechodu od kladně orientované báze $(\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k})$ k bázi $(\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{u} \times \boldsymbol{v})$. Její determinant spočítáme rozvojem podle třetího sloupce:

$$\det \mathbf{A} = \begin{vmatrix} u_2 & u_3 \\ v_2 & v_3 \end{vmatrix}^2 + \begin{vmatrix} u_1 & u_3 \\ v_1 & v_3 \end{vmatrix}^2 + \begin{vmatrix} u_1 & u_2 \\ v_1 & v_2 \end{vmatrix}^2 > 0.$$

Je tedy i báze $(\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{u} \times \boldsymbol{v})$ kladně orientovaná.

9.21. Poznámka. Věta 9.20 nám nejen dává možnost počítat souřadnice vektorového součinu ze souřadnic vstupních vektorů, ale inspiruje nás k definici vektorového součinu na $\mathbf{R}^3$:

9.22. Definice. Nechť $\boldsymbol{u} \in \mathbf{R}^3$, $\boldsymbol{v} \in \mathbf{R}^3$, $\boldsymbol{u} = (u_1, u_2, u_3)$, $\boldsymbol{v} = (v_1, v_2, v_3)$. Pak definujeme *vektorový součin na* $\mathbf{R}^3$ předpisem:

$$\boldsymbol{u} \times \boldsymbol{v} = \left(\begin{vmatrix} u_2 & u_3 \\ v_2 & v_3 \end{vmatrix}, - \begin{vmatrix} u_1 & u_3 \\ v_1 & v_3 \end{vmatrix}, \begin{vmatrix} u_1 & u_2 \\ v_1 & v_2 \end{vmatrix} \right).$$

9.23. Poznámka. Definici vektorového součinu lze rozšířit na libovolný lineární prostor L dimenze 3 se skalárním součinem, který byl orientován. Stačí použít definici 9.17 a uvědomit si, že se tato definice neopírá o žádné speciální vlastnosti množiny U_O. Vychází pouze z těchto předpokladů:

(1) Dimenze lineárního prostoru L musí být rovna třem.
(2) Na lineárním prostoru L musí být definován skalární součin.
(3) Lineární prostor L musí být orientován.

Rovněž důkaz věty 9.20 se opíral jen o výše uvedené vlastnosti lineárního prostoru a věta tedy platí pro každý takový lineární prostor.

Je třeba si uvědomit, že definici vektorového součinu nelze rozšířit na lineární prostory jiných dimenzí než 3.

9.24. Věta (základní vlastnosti vektorového součinu). Nechť L je lineární prostor s vektorovým součinem a $\boldsymbol{u} \in L$, $\boldsymbol{v} \in L$, $\boldsymbol{w} \in L$, $\alpha \in \mathbf{R}$. Platí:

$$\begin{aligned} \boldsymbol{u} \times \boldsymbol{u} &= \boldsymbol{o}, \\ \boldsymbol{u} \times \boldsymbol{v} &= -(\boldsymbol{v} \times \boldsymbol{u}) \qquad \text{(antikomutativní zákon)}, \\ (\alpha\, \boldsymbol{u}) \times \boldsymbol{v} &= \alpha\, (\boldsymbol{u} \times \boldsymbol{v}) = \boldsymbol{u} \times (\alpha\, \boldsymbol{v}), \\ (\boldsymbol{u} + \boldsymbol{v}) \times \boldsymbol{w} &= \boldsymbol{u} \times \boldsymbol{w} + \boldsymbol{v} \times \boldsymbol{w} \qquad \text{(první distributivní zákon)}, \\ \boldsymbol{u} \times (\boldsymbol{v} + \boldsymbol{w}) &= \boldsymbol{u} \times \boldsymbol{v} + \boldsymbol{u} \times \boldsymbol{w} \qquad \text{(druhý distributivní zákon)}. \end{aligned}$$

Důkaz. Snadno se dá ověřit, že tyto vzorce platí, pokud si zvolíme nějakou uspořádanou kladně orientovanou ortonormální bázi a budeme pracovat podle věty 9.20 se souřadnicemi těchto vektorů vzhledem k takto zvolené bázi.

9.25. Poznámka. Asociativní zákon pro vektorový součin neplatí, protože je $(\boldsymbol{i} \times \boldsymbol{i}) \times \boldsymbol{j} = \boldsymbol{o} \times \boldsymbol{j} = \boldsymbol{o}$, zatímco $\boldsymbol{i} \times (\boldsymbol{i} \times \boldsymbol{j}) = \boldsymbol{i} \times \boldsymbol{k} = -\boldsymbol{j}$, kde $(\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k})$ je uspořádaná kladně orientovaná ortonormální báze. Nemá tedy smysl psát $\boldsymbol{u} \times \boldsymbol{v} \times \boldsymbol{w}$ bez použití závorek. Při opakovaném vektorovém součinu vždy musíme pomocí závorek vyznačit, v jakém pořadí budeme násobit.

9.26. Příklad. Spočítáme $(2\boldsymbol{u} - 5\boldsymbol{v}) \times (\boldsymbol{u} + 3\boldsymbol{v})$ s využitím věty 9.24:

$$\begin{aligned} (2\boldsymbol{u} - 5\boldsymbol{v}) \times (\boldsymbol{u} + 3\boldsymbol{v}) &= (2\boldsymbol{u} - 5\boldsymbol{v}) \times \boldsymbol{u} + (2\boldsymbol{u} - 5\boldsymbol{v}) \times (3\boldsymbol{v}) = \\ &= (2\boldsymbol{u}) \times \boldsymbol{u} + (-5\boldsymbol{v}) \times \boldsymbol{u} + (2\boldsymbol{u}) \times (3\boldsymbol{v}) + (-5\boldsymbol{v}) \times (3\boldsymbol{v}) = \\ &= 2\,(\boldsymbol{u} \times \boldsymbol{u}) - 5\,(\boldsymbol{v} \times \boldsymbol{u}) + 6\,(\boldsymbol{u} \times \boldsymbol{v}) - 15\,(\boldsymbol{v} \times \boldsymbol{v}) = \\ &= 2\,\boldsymbol{o} - 5\,(-(\boldsymbol{u} \times \boldsymbol{v})) + 6\,(\boldsymbol{u} \times \boldsymbol{v}) - 15\,\boldsymbol{o} = 11\,(\boldsymbol{u} \times \boldsymbol{v}). \end{aligned}$$

9.27. Věta (geometrický význam vektorového součinu). Nechť vektory $\boldsymbol{u}, \boldsymbol{v}$ jsou lineárně nezávislé. Velikost vektorového součinu $\boldsymbol{u} \times \boldsymbol{v}$ je rovna ploše rovnoběžníka určeného svými stranami $\boldsymbol{u}$ a $\boldsymbol{v}$.

Důkaz. Stačí si uvědomit, že číslo $\|\boldsymbol{v}\| \sin\varphi$ (kde φ je úhel mezi vektory $\boldsymbol{u}$, $\boldsymbol{v}$) je rovno podle vlastnosti funkce sinus výšce zmíněného rovnoběžníka a $\|\boldsymbol{u}\|$ je jeho základna. Na základní škole jsme se učili, že plocha rovnoběžníka se počítá jako základna krát výška, tedy $\|\boldsymbol{u}\|\,\|\boldsymbol{v}\| \sin\varphi$, což je podle vlastnosti (2) definice 9.17 rovno velikosti vektorového součinu.

9.28. Definice. Nechť $\boldsymbol{u}$, $\boldsymbol{v}$, $\boldsymbol{w}$ jsou vektory z lineárního prostoru se skalárním a vektorovým součinem. Pak číslo $\boldsymbol{u} \cdot (\boldsymbol{v} \times \boldsymbol{w})$ nazýváme *smíšeným součinem vektorů* $\boldsymbol{u}$, $\boldsymbol{v}$, $\boldsymbol{w}$ *(v tomto pořadí).* *Smíšený součin*

9.29. Věta (smíšený součin ze souřadnic vektorů). Nechť $(B) = (\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k})$ je ortonormální kladně orientovaná uspořádaná báze lineárního prostoru se skalárním a vektorovým součinem, $\boldsymbol{u} = (u_1, u_2, u_3)_{(B)}$, $\boldsymbol{v} = (v_1, v_2, v_3)_{(B)}$, $\boldsymbol{w} = (w_1, w_2, w_3)_{(B)}$. Pak je smíšený součin $\boldsymbol{u} \cdot (\boldsymbol{v} \times \boldsymbol{w})$ roven determinantu:

$$\begin{vmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \\ w_1 & w_2 & w_3 \end{vmatrix}.$$

Důkaz. Věta plyne přímo z definice smíšeného součinu a vět 9.20, 8.33. Rozvojem determinantu podle prvního řádku dostáváme požadovaný výsledek.

9.30. Věta (geometrický význam smíšeného součinu). Absolutní hodnota smíšeného součinu lineárně nezávislých vektorů $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$ je rovna objemu rovnoběžnostěnu určeného svými stranami $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$.

Důkaz. Velikost vektorového součinu $\boldsymbol{v} \times \boldsymbol{w}$ je podle věty 9.27 roven ploše základny rovnoběžnostěnu. Rozepíšeme skalární součin pomocí kosinu úhlu φ mezi vektorem $\boldsymbol{u}$ a vektorem $\boldsymbol{v} \times \boldsymbol{w}$:

$$\|\boldsymbol{u} \cdot (\boldsymbol{v} \times \boldsymbol{w})\| = \|\boldsymbol{v} \times \boldsymbol{w}\| \cdot \|\boldsymbol{u}\| \, |\cos\varphi| = \text{základna} \cdot \text{výška} = \text{objem rovnoběžnostěnu}.$$

Číslo $\|\boldsymbol{u}\| \, |\cos\varphi|$ je rovno požadované výšce, protože se jedná o velikost kolmého průmětu vektoru $\boldsymbol{u}$ na vektor $\boldsymbol{v} \times \boldsymbol{w}$ a vektor $\boldsymbol{v} \times \boldsymbol{w}$ je kolmý na základnu.

9.31. Poznámka. Je-li báze $(\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w})$ kladně orientovaná, vychází smíšený součin kladně, protože úhel φ z důkazu předchozí věty je menší než $\pi/2$. Je-li ale tato báze záporně orientovaná, vychází smíšený součin jako záporné číslo, neboť úhel φ je větší než $\pi/2$.

9.32. Poznámka. Dá se ukázat, že absolutní hodnota determinantu matice typu (n, n) určuje objem rovnoběžnostěnu, který je určen svými stranami, jejichž souřadnice jsou zapsány do řádků této matice. Rovnoběžnostěn se „rozprostírá“ v n-dimenzionálním prostoru. Pomocí determinantů tedy můžeme měřit n-dimenzionální objemy. Věty 9.29 a 9.30 ilustrují, že determinanty měří objemy rovnoběžnostěnu aspoň pro dimenzi 3.

Prostor V_3 volných vektorů

9.33. Poznámka. Lineární prostor U_O z příkladů 9.2, 9.3 a 9.7 má jednu nevýhodu. Obsahuje jen úsečky, které začínají v pevně zvoleném bodě O. Často ale při modelování fyzikálních situací ztotožňujeme orientovanou úsečku s jinou, která začíná v jiném bodě, ale je s původní úsečkou rovnoběžná, má stejnou velikost a stejnou orientaci.

Z tohoto důvodu je výhodné zavést lineární prostor tzv. *volných vektorů* V_3, ve kterém budeme ztotožňovat dvě úsečky, pokud jsou rovnoběžné, mají stejnou velikost a jsou stejně orientované.

9.34. Definice. Nechť U_O je lineární prostor z příkladů 9.2 a 9.3. Volme $\boldsymbol{u}_O \in U_O$. Množinu všech orientovaných úseček, které jsou s úsečkou $\boldsymbol{u}_O$ rovnoběžné a mají stejnou velikost a orientaci nazýváme *vektorem lineárního prostoru* V_3.

Nechť $\boldsymbol{u}$ je vektor lineárního prostoru V_3 Jde tedy o množinu vzájemně rovnoběžných úseček stejně velkých a stejně orientovaných. Jakoukoli orientovanu úsečku z této množiny nazýváme *reprezentantem vektoru* $\boldsymbol{u}$.

Na lineárním prostoru V_3 definujeme sčítání vektorů a skalární násobek. Nechť $\boldsymbol{u} \in V_3$, $\boldsymbol{v} \in V_3$. Volme nějaký bod $O \in \mathbf{E}_3$. Existuje právě jeden reprezentant vektoru $\boldsymbol{u}$, který začíná v bodě O. Označme jej $\boldsymbol{u}_O$. Dále nechť $\boldsymbol{v}_O$ je reprezentant vektoru $\boldsymbol{v}$ začínající v bodě O. Pak je definován součet $\boldsymbol{w}_O = \boldsymbol{u}_O + \boldsymbol{v}_O$ na lineárním prostoru U_O. Součet $\boldsymbol{u} + \boldsymbol{v}$ je takový prvek z V_3, pro který je $\boldsymbol{w}_O$ jeho reprezentantem začínajícím v bodě O. Je to tedy množina všech orientovaných úseček rovnoběžných, stejně velkých a stejně orientovaných, jako úsečka $\boldsymbol{w}_O$.

Skalární násobek definujeme podobně. Nechť je $\boldsymbol{u} \in V_3$, $\alpha \in \mathbf{R}$. Pro $\boldsymbol{u}$ existuje reprezentant $\boldsymbol{u}_O$ začínající v bodě O. K němu existuje skalární násobek definovaný v U_O. Označme jej $\boldsymbol{w}_O = \alpha\, \boldsymbol{u}_O$. Výsledný vektor $\alpha\, \boldsymbol{u}$ je vektorem z V_3 takovým, že $\boldsymbol{w}_O$ je jeho reprezentant.

Skalární součin vektorů $\boldsymbol{u} \in V_3$, $\boldsymbol{v} \in V_3$ definujeme jako skalární součin jejich reprezentantů $\boldsymbol{u}_O$ a $\boldsymbol{v}_O$ v lineárním prostoru U_O.

Vektorový součin $\boldsymbol{u} \times \boldsymbol{v}$ definujeme tak, že reprezentanty $\boldsymbol{u}_O$ a $\boldsymbol{v}_O$ vektorů $\boldsymbol{u}$ a $\boldsymbol{v}$ vynásobíme v lineárním prostoru U_O. Výsledný součin $\boldsymbol{u} \times \boldsymbol{v}$ je takový vektor, pro který je $\boldsymbol{u}_O \times \boldsymbol{v}_O$ jeho reprezentantem začínajícím v bodě O.

9.35. Poznámka. Dá se snadno ukázat, že výše definovaný součet, skalární násobek, skalární součin a vektorový součin vektorů z V_3 nejsou závislé na volbě bodu $O \in \mathbf{E}_3$.

9.36. Poznámka. Volme pevně bod $O \in \mathbf{E}_3$. Uvažujme zobrazení, které každému vektoru $\boldsymbol{u}_O \in U_O$ přiřadí $\boldsymbol{u} \in V_3$ tak, že $\boldsymbol{u}_O$ je reprezentantem vektoru $\boldsymbol{u}$ začínajícím v bodě O. Toto zobrazení je prosté a na. Navíc je lineární. Jedná se tedy o izomorfismus. Všechny pojmy, které jsme definovali na U_O lze prostřednictvím tohoto izomorfismu definovat i na lineárním prostoru V_3. Například:

9.37. Definice. *Ortonormální báze na* V_3 je taková báze, jejíž reprezentanti začínající v nějakém bodě $O \in \mathbf{E}_3$ tvoří ortonormální bázi v U_O. Viz příklad 9.7.

Kladně orientovaná báze na V_3 ja taková báze, jejíž reprezentanti začínající v nějakém bodě $O \in \mathbf{E}_3$ tvoří kladně orientovanou bázi v U_O. Viz definici 9.10.

9.38. Poznámka. Pro potřeby popisů geometrických objektů se kromě součtu volných vektorů mezi sebou hodí definovat součet bodu s volným vektorem a rozdíl bodů. *Součet bodu s vektorem*

9.39. Definice. Pro každý bod $A \in \mathbf{E}_3$ a volný vektor $\boldsymbol{v} \in V_3$ existuje právě jeden reprezentant vektoru $\boldsymbol{v}$, který začíná v bodě A. Koncový bod $B \in \mathbf{E}_3$ tohoto reprezentanta nazýváme *součtem bodu A s vektorem $\boldsymbol{v}$* a značíme $B = A + \boldsymbol{v}$.

Pro každé dva body $A \in \mathbf{E}_3$, $B \in \mathbf{E}_3$ existuje $\boldsymbol{v} \in V_3$ takový, že orientovaná úsečka s počátkem v bodě A a koncem v bodě B je reprezentantem tohoto vektoru. Vektor $\boldsymbol{v}$ nazýváme *rozdílem $B - A$*, píšeme $\boldsymbol{v} = B - A$. Vektor $B - A$ se často značí symbolem $\overrightarrow{AB}$.

9.40. Poznámka. Shrneme si, co s čím můžeme sčítat a s jakým výsledkem:

$$\begin{aligned} \text{volný vektor} \pm \text{volný vektor} &= \text{volný vektor}, \\ \text{bod} \pm \text{volný vektor} &= \text{bod}, \\ \text{bod} + \text{bod} &\ldots \textit{nemá smysl}, \\ \text{bod} - \text{bod} &= \text{volný vektor}. \end{aligned}$$

Definice sčítání bodu s vektorem a odčítání bodů se vzájemně doplňují, tj. platí $A + (B - A) = B$.

9.41. Příklad. V návaznosti na příklad 9.2 a definici 9.39 dostáváme následující popisy přímek a rovin v bodovém prostoru $\mathbf{E}_3$. *Přímka a rovina*

Nechť $\boldsymbol{u} \in V_3$ je nenulový vektor, $A \in \mathbf{E}_3$. Pak

$$p = A + \langle \boldsymbol{u} \rangle = \{X \in \mathbf{E}_3;\ X = A + t\,\boldsymbol{u},\ t \in \mathbf{R}\}$$

je přímka v bodovém prostoru $\mathbf{E}_3$, která prochází bodem A a je rovnoběžná se všemi reprezentanty vektoru $\boldsymbol{u}$. Vektor $\boldsymbol{u}$ se nazývá *směrovým vektorem* přímky p.

Nechť dále $\{\boldsymbol{u}, \boldsymbol{v}\} \subset V_3$ jsou lineárně nezávislé vektory. Pak

$$\varrho = A + \langle \boldsymbol{u}, \boldsymbol{v} \rangle = \{X \in \mathbf{E}_3;\ X = A + r\,\boldsymbol{u} + s\,\boldsymbol{v},\ r \in \mathbf{R},\ s \in \mathbf{R}\}$$

je rovina v bodovém prostoru $\mathbf{E}_3$, která prochází bodem A. Navíc reprezentanti vektorů $\boldsymbol{u}$ a $\boldsymbol{v}$ s počátkem v bodě A leží uvnitř této roviny. Vektorům $\boldsymbol{u}$, $\boldsymbol{v}$ říkáme *směrové vektory roviny.*

Existuje nekonečně mnoho bodů a nekonečně mnoho směrových vektorů, pomocí kterých je určena stejná přímka resp. stejná rovina. S touto nejednoznačností jsme se už setkali při řešení soustav lineárních rovnic v poznámkách 5.25 a 5.26.

9.42. Definice. Libovolný bod $O \in \mathbf{E}_3$ společně s uspořádanou bází $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ vektorů z V_3 tvoří *souřadnicový systém bodového prostoru* $\mathbf{E}_3$. *Souřadnicový systém v* $\mathbf{E}_3$

Souřadnice vektoru $\boldsymbol{u} \in V_3$ v tomto souřadnicovém systému definujeme jako souřadnice vektoru $\boldsymbol{u}$ vzhledem k uspořádané bázi (B).

Souřadnice bodu $A \in \mathbf{E}_3$ v tomto souřadnicovém systému definujeme jako souřadnice vektoru $A - O$. Vektor $A - O$ nazýváme v tomto kontextu *radiusvektorem bodu A.*

Přímky $O + \langle \boldsymbol{b}_1 \rangle$, $O + \langle \boldsymbol{b}_2 \rangle$, $O + \langle \boldsymbol{b}_3 \rangle$ jsou *osy souřadnicového systému.*

Je-li báze (B) ortogonální, nazýváme odpovídající souřadnicový systém *pravoúhlý.* Je-li báze (B) ortonormální, nazýváme odpovídající souřadnicový systém *kartézský.* Je-li báze (B) kladně orientovaná, mluvíme též o *kladně orientovaném souřadnicovém systému.*

9.43. Poznámka. Uvědomíme si podrobně, co to znamená, že bod A má souřadnice (a_1, a_2, a_3) vzhledem k nějakému souřadnicovému systému $(O, (\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3))$. Podle výše uvedené definice to znamená, že vektor $A - O$ má souřadnice (a_1, a_2, a_3), což podle definice souřadnic vektoru vzhledem k bázi znamená, že

$$(A - O) = a_1\boldsymbol{b}_1 + a_2\boldsymbol{b}_2 + a_3\boldsymbol{b}_3.$$

9.44. Věta. Zvolme pevně souřadnicový systém bodového prostoru $\mathbf{E}_3$, vzhledem ke kterému budeme udávat souřadnice bodů a vektorů. Tento souřadnicový systém nemusí být nutně kartézský. Nechť $A \in \mathbf{E}_3$ má souřadnice (a_1, a_2, a_3), $B \in \mathbf{E}_3$ má souřadnice (b_1, b_2, b_3), $\boldsymbol{u} \in V_3$ má souřadnice (u_1, u_2, u_3), $\boldsymbol{v} \in V_3$ má souřadnice (v_1, v_2, v_3), $\alpha \in \mathbf{R}$, $\beta \in \mathbf{R}$. Potom platí:

(1) Vektor $\alpha\,\boldsymbol{u} + \beta\,\boldsymbol{v}$ má souřadnice $\alpha\,(u_1, u_2, u_3) + \beta\,(v_1, v_2, v_3)$.
(2) Bod $A + \boldsymbol{u}$ má souřadnice $(a_1, a_2, a_3) + (u_1, u_2, u_3)$.
(3) Vektor $\overrightarrow{AB} = B - A$ má souřadnice $(b_1, b_2, b_3) - (a_1, a_2, a_3)$.

Důkaz. Ad (1). Zobrazení, které přiřadí vektorům jejich souřadnice je podle příkladu 7.25 lineární.
Ad (2). $(A - O) + \boldsymbol{u}$ je radiusvektor bodu $A + \boldsymbol{u}$. Dále se použije vlastnost (1).
Ad (3). Využijeme například toho, že $A + (B - A) = B$.

9.45. Poznámka. Protože podle předchozí věty se operace sčítání bodů s vektory dají převést na operace sčítání uspořádaných trojic jejich souřadnic, bývá často zvykem ztotožnit body z $\mathbf{E}_3$ a vektory z V_3 s uspořádanými trojicemi jejich souřadnic. Píšeme tedy například $A = (1, 2, -5)$ a čteme, že bod A má souřadnice $(1, 2, -5)$.

V jiné literatuře (např. [7]) se skutečnost, že bod A má dány souřadnice, zapisuje bez rovnítka a do hranatých závorek. Náš příklad se souřadnicemi $(1, 2, -5)$ by vypadal takto: $A[1, 2, -5]$. Osobně toto značení nemám v oblibě, protože mezi označením bodu A a jeho souřadnicemi $[1, 2, -5]$ chybí symbol pro sloveso.

9.46. Příklad. Vypočteme vzdálenost dvou bodů $A \in \mathbf{E}_3$ a $B \in \mathbf{E}_3$, pokud známe jejich souřadnice v kartézském souřadnicovém systému.

Vzdálenost bodů A a B je rovna velikosti vektoru $B - A$ a tu spočítáme podle definice velikosti jako $\sqrt{(B - A) \cdot (B - A)}$. Přitom skalární součin spočítáme podle věty 8.33.

Uvedeme konkrétní příklad. Nechť $A = (1, 2, -5)$, $B = (3, 2, 1)$. Vzdálenost těchto bodů je rovna velikosti vektoru $B - A$, který má podle věty 9.44 souřadnice $(2, 0, 6)$. Počítáme velikost:

$$\|(2, 0, 6)\| = \sqrt{(2, 0, 6) \cdot (2, 0, 6)} = \sqrt{2^2 + 0^2 + 6^2} = \sqrt{40}.$$

Uvedený postup s použitím věty 8.33 lze použít jen pro souřadnice v kartézském souřadnicovém systému, protože tato věta předpokládá souřadnice vektoru vzhledem k ortonormální bázi.

9.47. Příklad. Vypočteme obsah trojúhelníka v bodovém prostoru $\mathbf{E}_3$, pokud jsou dány kartézské souřadnice jeho vrcholů A, B, C.

Podle věty 9.27 je obsah rovnoběžníka roven velikosti vektorového součinu jeho stran. Trojúhelník pak bude mít obsah poloviční. Obsah trojúhelníka tedy můžeme počítat takto:

$$P = \frac{\|(B - A) \times (C - A)\|}{2}.$$

Jsou-li dány kartézské souřadnice vrcholů třeba takto: $A = (1, 2, 2)$, $B = (2, -3, 3)$, $C = (1, 4, 5)$, pak stačí dosadit do právě odvozeného vzorce:

$$P = \frac{\|\big((2, -3, 3) - (1, 2, 2)\big) \times \big((1, 4, 5) - (1, 2, 2)\big)\|}{2} = \frac{\|(1, -5, 1) \times (0, 2, 3)\|}{2} =$$
$$= \frac{\|(-17, -3, 2)\|}{2} = \frac{\sqrt{17^2 + 3^2 + 2^2}}{2} = \frac{\sqrt{302}}{2}.$$

Při výpočtu jsme použili nejen věty 9.44, ale též věty 9.20 pro výpočet vektorového součinu ze souřadnic a věty 8.33 pro výpočet skalárního součinu, který jsme potřebovali na výpočet velikosti vektoru. Posledně zmíněné věty předpokládají souřadnice vzhledem k ortonormální bázi, a proto bylo nutné mít souřadnice bodů zadány v *kartézském* systému souřadnic.

9.48. Příklad. Vypočteme objem čtyřstěnu, určeného vrcholy A, B, C, D. Tyto vrcholy jsou dány v kartézských souřadnicích.

Podle vět 9.29 a 9.30 je objem rovnoběžnostěnu roven absolutní hodnotě z determinantu, ve kterém jsou v řádcích napsány souřadnice jeho stran. Čtyřstěn bude mít objem šestinový, protože do rovnoběžnostěnu se vejde právě šest čtyřstěnů se shodným objemem. Kdo o tom pochybuje, rozkrájí si za domácí cvičení kostku tvrdého sýra na šest čtyřstěnů se stejným objemem.

Nechť $\mathbf{A}$ je matice, která má v prvním řádku souřadnice vektoru $B-A$, ve druhém řádku souřadnice $C-A$ a ve třetím řádku souřadnice $D-A$. Pak objem čtyřstěnu V je roven $|\det \mathbf{A}|/6$.

Věta 9.29 předpokládá ortonormální bázi, proto je potřeba pracovat se souřadnicemi bodů v *kartézském* systému souřadnic.

9.49. Příklad. Ukážeme si, jak popíšeme přímku v souřadnicovém systému. Podle příkladu 9.41 a věty 9.44 je přímka p procházející bodem $A = (a_1, a_2, a_3)$ se směrovým vektorem $\boldsymbol{u} = (u_1, u_2, u_3)$ množinou takových bodů $X = (x, y, z)$, pro které platí: *Rovnice přímky*

$$X = A + t\,\boldsymbol{u},\ t \in \mathbf{R} \quad \text{tj.} \quad (x, y, z) = (a_1, a_2, a_3) + t\,(u_1, u_2, u_3), t \in \mathbf{R}.$$

Po rozepsání této rovnosti do jednotlivých souřadnic dostáváme *parametrické rovnice přímky*:

$$\begin{aligned} x &= a_1 + t\,u_1, \\ y &= a_2 + t\,u_2, \\ z &= a_3 + t\,u_3. \end{aligned}$$

Pokud vypočítáme z každé rovnice parametr t a výsledky položíme sobě rovny, dostáváme tzv. *kanonickou rovnici přímky*:

$$\frac{x - a_1}{u_1} = \frac{y - a_2}{u_2} = \frac{z - a_3}{u_3}.$$

9.50. Příklad. Popíšeme přímku, která prochází body $A = (1, 2, 3)$ a $B = (2, 2, 0)$.

Směrovým vektorem přímky je například vektor $B - A = (1, 0, -3)$ a přímka má tvar:

$$p = A + \langle B{-}A \rangle = (1, 2, 3) + \langle (1, 0, -3) \rangle = \big\{(x, y, z);\ (x, y, z) = (1, 2, 3) + t\,(1, 0, -3),\ t \in \mathbf{R}\big\}.$$

Odtud dostáváme parametrické rovnice přímky:

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

a kanonický tvar:

$$\frac{x - 1}{1} = \frac{y - 2}{0} = \frac{z - 3}{-3}.$$

Na zlomky v kanonickém tvaru pohlížíme jako na formální zápisy a nepozastavujeme se nad tím, že se tam může vyskytnout dělení nulou. Kanonický tvar nám poskytuje informaci o souřadnicích směrového vektoru ve jmenovatelích zlomků a souřadnice bodu $A \in p$ přečteme v čitatelích zlomků.

9.51. Příklad. Ukážeme, jak spočítáme vzdálenost bodu $Q \in \mathbf{E}_3$ od přímky $p = A + \langle \boldsymbol{u} \rangle$.

Tato vzdálenost je rovna výšce rovnoběžníka určeného stranami $Q - A$ a $\boldsymbol{u}$. Základna tohoto rovnoběžníka má velikost $\|\boldsymbol{u}\|$. Platí tedy:

$$\text{vzdálenost bodu } Q \text{ od přímky } p = \text{výška rovnoběžníka} = \frac{\text{obsah rovnoběžníka}}{\text{velikost základny}} = \frac{\|(Q - A) \times \boldsymbol{u}\|}{\|\boldsymbol{u}\|}.$$

Vzájemná poloha dvou přímek

9.52. Příklad. Vyšetříme vzájemnou polohu dvou přímek $p = A + \langle \boldsymbol{u} \rangle$ a $q = B + \langle \boldsymbol{v} \rangle$.

Jsou-li vektory $\boldsymbol{u}, \boldsymbol{v}, B-A$ lineárně nezávislé, pak přímky neleží ve společné rovině a jsou tedy *mimoběžné*. Níže ukážeme, jak vypočítáme vzdálenost těchto přímek.

Jsou-li vektory $\boldsymbol{u}, \boldsymbol{v}, B-A$ lineárně závislé, pak přímky leží ve společné rovině a mohou být různoběžné, rovnoběžné nebo totožné. Jsou-li v takovém případě vektory $\boldsymbol{u}, \boldsymbol{v}$ lineárně nezávislé, jsou přímky *různoběžné*. Níže ukážeme, jak vypočítáme průsečík a úhel mezi různoběžkami. Jsou-li konečně vektory $\boldsymbol{u}, \boldsymbol{v}$ lineárně závislé, jedná se o *rovnoběžky* a v případě, že bod $B \in p$, pak tyto rovnoběžky splývají v přímku jedinou. Níže ukážeme, jak vypočítáme vzdálenost rovnoběžek.

Vzdálenost dvou mimoběžek počítáme z objemu rovnoběžnostěnu, určeného svými stranami $\boldsymbol{u}, \boldsymbol{v}, B-A$, který z jedné strany lze počítat jako absolutní hodnotu smíšeného součinu a z druhé strany je tento objem roven obsahu rovnoběžníka základny krát výška. Tato výška je přitom hledaná vzdálenost. Platí tedy:

$$\text{vzdálenost mimoběžek} = \frac{\text{objem rovnoběžnostěnu}}{\text{obsah základny}} = \frac{|(B-A)\cdot(\boldsymbol{u}\times\boldsymbol{v})|}{\|\boldsymbol{u}\times\boldsymbol{v}\|} = \frac{|\det \mathbf{A}|}{\|\boldsymbol{u}\times\boldsymbol{v}\|}, \tag{9.3}$$

kde matice $\mathbf{A}$ obsahuje postupně řádky se souřadnicemi vektorů $B-A$, $\boldsymbol{u}$, $\boldsymbol{v}$.

Vzdálenost rovnoběžek vypočítáme jako vzdálenost bodu na jedné rovnoběžce od rovnoběžky druhé. To jsme dělali v příkladu 9.51. Máme tedy už odvozený vzorec:

$$\text{vzdálenost rovnoběžek} = \frac{\|(B-A)\times\boldsymbol{u}\|}{\|\boldsymbol{u}\|}.$$

Úhel mezi různoběžkami je roven úhlu φ mezi vektory $\boldsymbol{u}$, $\boldsymbol{v}$, který spočítáme podle definice 8.20. Může se ale stát, že tento úhel vychází větší než $\pi/2$. V takovém případě je úhel mezi přímkami roven $\pi-\varphi$. Tento vzorec vyplývá z toho, že mezi různoběžkami můžeme měřit dva úhly a za „oficiální" úhel mezi nimi považujeme ten menší z nich. Protože platí $|\cos\varphi| = \cos\varphi$ pro $0 \le \varphi \le \pi/2$ a $|\cos\varphi| = \cos(\pi-\varphi)$ pro $\pi/2 < \varphi \le \pi$, můžeme oba případy zahrnout do jediného vzorce, ve kterém píšeme absolutní hodnotu skalárního součinu:

$$\cos\varphi = \frac{|\boldsymbol{u}\cdot\boldsymbol{v}|}{\|\boldsymbol{u}\|\,\|\boldsymbol{v}\|}. \tag{9.4}$$

Souřadnice průsečíku různoběžek spočítáme jako společné řešení parametrických rovnic jednak pro přímku p a jednak pro přímku q.

9.53. Příklad. Vyšetříme vzájemnou polohu přímek p a q, které jsou dány svými parametrickými rovnicemi v kartézském souřadnicovém systému:

$$p:\ \begin{array}{l} x = 1 + t \\ y = \phantom{1+{}} 2t \\ z = 2 \end{array} \qquad q:\ \begin{array}{l} x = 3 + t \\ y = 2 \\ z = 1 - t \end{array}.$$

Z rovnic okamžitě vidíme souřadnice bodu, kterým přímka prochází a souřadnice směrového vektoru:

$$p = (1,0,2) + \langle (1,2,0) \rangle, \qquad q = (3,2,1) + \langle (1,0,-1) \rangle.$$

Při označení $A = (1,0,2)$, $B = (3,2,1)$ je $B - A = (2,2,-1)$. Zjistíme lineární závislost vektoru $B - A$ a směrových vektorů tak, že zapíšeme souřadnice těchto vektorů do matice a počítáme determinant:

$$\begin{vmatrix} 2 & 2 & -1 \\ 1 & 2 & 0 \\ 1 & 0 & -1 \end{vmatrix} = 0. \tag{9.5}$$

Zkoumané vektory jsou lineárně závislé, přímky tedy leží ve společné rovině. Protože směrové vektory $(1,2,0)$, $(1,0,-1)$ jsou lineárně nezávislé, p, q jsou *různoběžky*.

Úhel mezi různoběžkami počítáme podle vzorce (9.4):

$$\cos\varphi = \frac{|(1,2,0)\cdot(1,0,-1)|}{\|(1,2,0)\|\,\|(1,0,-1)\|} = \frac{|1+0+0|}{\sqrt{1^2+2^2+0^2}\sqrt{1^1+0^2+1^2}} = \frac{1}{\sqrt{10}}, \quad \text{tj.} \quad \varphi = \arccos\frac{1}{\sqrt{10}}.$$

Průsečík vychází z rovnic $x = x$, $y = y$, $z = z$, kde za souřadnice x, y, z dosadíme pravé strany odpovídajících parametrických rovnic a u přímky q zvolíme pro parametr jiné označení:

$$\begin{aligned} 1 + t &= 3 + s \\ 2t &= 2 \\ 2 &= 1 - s \end{aligned}$$

Soustava je sice „přeurčena“ (je zde více rovnic než neznámých), ale protože nám vyšel determinant (9.5) nulový, má tato soustava určitě řešení. Řešením je v tomto případě $t = 1$, $s = -1$. Dosazením třeba $t = 1$ do parametrických rovnic přímky p dostáváme souřadnice průsečíku: $P = (1, 0, 2) + 1 \cdot (1, 2, 0) = (2, 2, 2)$.

9.54. Příklad. Vyšetříme vzájemnou polohu přímky p procházející body A, B s přímkou q procházející body C, D. Body jsou dány v kartézských souřadnicích takto: $A = (1, 2, 3)$, $B = (3, 2, 1)$, $C = (1, 0, 2)$, $D = (4, 2, 3)$.

Směrový vektor přímky p je třeba $B - A = (2, 0, -2) \sim (1, 0, -1)$. Za vlnkou jsme napsali sice jiný směrový vektor, ale je to rovněž směrový vektor přímky p a navíc má souřadnice, se kterými se nám bude pohodlněji pracovat. Směrový vektor přímky q je třeba $D - C = (3, 2, 1)$. Máme tedy:

$$p = (1, 2, 3) + \langle (1, 0, -1) \rangle, \qquad q = (1, 0, 2) + \langle (3, 2, 1) \rangle.$$

Snadno ověříme, že vektory $A - C, (1, 0, -1), (3, 2, 1)$ jsou lineárně nezávislé, takže přímky jsou *mimoběžné*. Determinant matice, obsahující souřadnice těchto vektorů, je roven -6. Vzdálenost mimoběžek počítáme podle vzorce (9.3):

$$\frac{|\det \mathbf{A}|}{\|(1, 0, -1) \times (3, 2, 1)\|} = \frac{|-6|}{\|(2, -4, 2)\|} = \frac{6}{\sqrt{2^2 + 4^2 + 2^2}} = \frac{6}{\sqrt{24}}.$$

9.55. Příklad. Ukážeme si, jak můžeme popsat rovinu ϱ v souřadnicovém systému. *Rovnice roviny*

Nechť je rovina ϱ určena bodem $A = (a_1, a_2, a_3)$, kterým prochází, a dvěma lineárně nezávislými směrovými vektory $\boldsymbol{u} = (u_1, u_2, u_3)$, $\boldsymbol{v} = (v_1, v_2, v_3)$. Podle příkladu 9.41 je rovina ϱ množinou takových bodů $X = (x, y, z)$, pro které platí:

$$X = A + t\,\boldsymbol{u} + s\,\boldsymbol{v}, t \in \mathbf{R}, s \in \mathbf{R}, \quad \text{tj.} \quad (x, y, z) = (a_1, a_2, a_3) + t\,(u_1, u_2, u_3) + s\,(v_1, v_2, v_3), t \in \mathbf{R}, s \in \mathbf{R}.$$

Rozepsáním do jednotlivých souřadnic nám vycházejí *parametrické rovnice roviny*:

$$\begin{aligned} x &= a_1 + t\,u_1 + s\,v_1 \\ y &= a_2 + t\,u_2 + s\,v_2 \\ z &= a_3 + t\,u_3 + s\,v_3 \end{aligned}$$

Na rozdíl od parametrických rovnic přímky se s parametrickými rovnicemi roviny moc často nesetkáme. Místo toho se pracuje s *normálovým vektorem roviny*, což je libovolný nenulový vektor $\boldsymbol{n}$, který je kolmý na rovinu ϱ. Rovina je určena jedním bodem $A = (a_1, a_2, a_3)$, kterým prochází, a normálovým vektorem $\boldsymbol{n} = (a, b, c)$. Rovina je pak množinou takových bodů $X = (x, y, z)$, pro které platí:

$$(X - A) \perp \boldsymbol{n}, \quad \text{tj.} \quad (X - A) \cdot \boldsymbol{n} = 0, \quad \text{tj.} \quad (x - a_1, y - a_2, z - a_3) \cdot (a, b, c) = 0.$$

V kartézském souřadnicovém systému můžeme pro výpočet skalárního součinu použít větu 8.33 a dostáváme *normálovou rovnici roviny*, nebo prostě jen *rovnici roviny*:

$$ax + by + cz + d = 0, \quad \text{kde} \quad d = -aa_1 - ba_2 - ca_3.$$

Uvědomíme si, že v rovnici roviny jsou přímo čitelné souřadnice normálového vektoru roviny $\boldsymbol{n} = (a, b, c)$, což je velmi užitečná informace.

9.56. Příklad. Ukážeme si, jak je možné přejít od směrových vektorů $\boldsymbol{u}$, $\boldsymbol{v}$ roviny ϱ k normálové rovnici roviny.

Protože směrové vektory $\boldsymbol{u}$ a $\boldsymbol{v}$ jsou lineárně nezávislé, je $\boldsymbol{n} = \boldsymbol{u} \times \boldsymbol{v}$ normálovým vektorem roviny. Je totiž podle definice vektorového součinu kolmý na oba vektory $\boldsymbol{u}$ a $\boldsymbol{v}$ a tedy je kolmý na celou rovinu ϱ. Abychom našli konstanty a, b, c použité v normálové rovnici roviny, stačí tedy vypočítat vektorový součin $\boldsymbol{u} \times \boldsymbol{v}$. Konstantu d dopočítáme buď ze skutečnosti, že je dán bod $A \in \mathbf{E}_3$, který v rovině leží, nebo vyhodnocením skalárního součinu jako v předchozím příkladu.

Existuje ještě jeden způsob sestavení normálové rovnice ze směrových vektorů $\boldsymbol{u}$, $\boldsymbol{v}$. Rovina ϱ, která prochází bodem $A \in \mathbf{E}_3$, je totiž také množinou bodů $X \in \mathbf{E}_3$, pro které je trojice vektorů $(X - A), \boldsymbol{u}, \boldsymbol{v}$ lineárně závislá. Jinými slovy pro matici, která obsahuje v řádcích souřadnice těchto vektorů, musí platit, že má nulový determinant. Při $A = (a_1, a_2, a_3)$, $\boldsymbol{u} = (u_1, u_2, u_3)$, $\boldsymbol{v} = (v_1, v_2, v_3)$, $X = (x, y, z)$ nám vychází:

$$\begin{vmatrix} x - a_1 & y - a_2 & z - a_3 \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{vmatrix} = 0.$$

Výpočtem tohoto determinantu dostáváme normálovou rovnici roviny.

9.57. Příklad. Najdeme rovnici roviny, která prochází body $A = (1, 2, 3)$, $B = (1, 1, 1)$, $C = (2, 0, 2)$.

Jedná se o rovinu, která prochází například bodem A a je určena směrovými vektory $B - A$, $C - A$. Jinými slovy

$$\varrho = A + \langle B - A, C - A \rangle = (1, 2, 3) + \langle (0, -1, -2), (1, -2, -1) \rangle.$$

Je tedy ϱ množina takových bodů $X = (x, y, z)$, pro které platí

$$(x, y, z) = (1, 2, 3) + t\,(0, -1, -2) + s\,(1, -2, -1),\ t \in \mathbf{R},\ s \in \mathbf{R}.$$

Odtud dostáváme parametrické rovnice roviny ϱ:

$$\begin{aligned} x &= 1 + s \\ y &= 2 - t - 2s \\ z &= 3 - 2t - s \end{aligned}$$

Normálový vektor roviny ϱ spočítáme jako vektorový součin směrových vektorů:

$$\boldsymbol{n} = (0, -1, -2) \times (1, -2, -1) = (-3, -2, 1).$$

Rovnice roviny má tedy tvar $-3x - 2y + z + d = 0$. Konstantu $d \in \mathbf{R}$ najdeme například na základě skutečnosti, že $A \in \varrho$, takže musí platit

$$-3 \cdot 1 - 2 \cdot 2 + 3 + d = 0, \quad \text{tj.} \quad d = 4 \quad \text{a rovnice roviny je:} \quad -3x - 2y + z + 4 = 0.$$

Druhý způsob sestavení rovnice roviny výpočtem determinantu vypadá takto:

$$\begin{vmatrix} x - 1 & y - 2 & z - 3 \\ 0 & -1 & -2 \\ 1 & -2 & -1 \end{vmatrix} = 0, \quad \text{tj.} \quad -3x - 2y + z + 4 = 0.$$

9.58. Příklad. Najdeme vzdálenost bodu $Q \in \mathbf{E}_3$ od roviny ϱ.

Nechť A je libovolný bod roviny ϱ. Vzdálenost bodu Q od roviny ϱ je rovna absolutní hodnotě kolmého průmětu vektoru $Q - A$ do normálového vektoru $\boldsymbol{n}$ roviny ϱ. Na výpočet velikosti kolmého průmětu vektoru použijeme skalární součin podle definice 9.6. Dostáváme:

$$\text{vzdálenost bodu od roviny} = \frac{|(Q - A) \cdot \boldsymbol{n}|}{\|\boldsymbol{n}\|}. \tag{9.6}$$

Nechť například $Q = (1, 4, 3)$ a rovina ϱ má rovnici $3x - 2y + 4z + 6 = 0$ v kartézských souřadnicích. Z rovnice roviny okamžitě vidíme souřadnice normálového vektoru $\boldsymbol{n} = (3, -2, 4)$. Musíme ještě najít aspoň jedno řešení rovnice roviny, abychom získali souřadnice bodu $A \in \varrho$. Při $x = 0$ a $z = 0$ vychází $y = 3$, takže použijeme bod $A = (0, 3, 0)$, $Q - A = (1, 1, 3)$. Hledaná vzdálenost je:

$$v = \frac{|(1, 1, 3) \cdot (3, -2, 4)|}{\|(3, -2, 4)\|} = \frac{|1 \cdot 3 + 1 \cdot (-2) + 3 \cdot 4|}{\sqrt{3^2 + 2^2 + 4^2}} = \frac{13}{\sqrt{29}}.$$

9.59. Příklad. Vyšetříme vzájemnou polohu přímky $p = A + \langle \boldsymbol{u} \rangle$ a roviny ϱ, která prochází daným bodem B a má normálový vektor $\boldsymbol{n}$.

Vzájemná poloha přímky a roviny

Je-li $\boldsymbol{u} \perp \boldsymbol{n}$, neboli $\boldsymbol{u} \cdot \boldsymbol{n} = 0$, pak je přímka rovnoběžná s rovinou. V takovém případě ještě může nastat situace, kdy celá přímka leží v rovině, což zjistíme například podle toho, že $(B - A) \perp \boldsymbol{n}$, neboli $(B - A) \cdot \boldsymbol{n} = 0$. Pokud je přímka rovnoběžná s rovinou, určíme vzdálenost přímky p od roviny ϱ stejně jako vzdálenost bodu $A \in p$ od roviny ϱ. To jsme se naučili v předchozím příkladě 9.58.

Je-li $\boldsymbol{u} \cdot \boldsymbol{n} \neq 0$, pak přímka p protíná rovinu ϱ v jediném bodě. Průsečík najdeme tak, že dosadíme hodnoty x, y, z z parametrických rovnic přímky do rovnice roviny. Tím dostaneme hodnotu parametru, který nám dá po dosazení do parametrických rovnic souřadnice hledaného průsečíku. Tento postup ilustrujeme v následujícím příkladě.

Úhel mezi přímkou p protínající rovinu ϱ a touto rovinou je roven $\alpha = \pi/2 - \varphi$, kde φ je úhel mezi směrovým vektorem přímky $\boldsymbol{u}$ a normálovým vektorem roviny $\boldsymbol{n}$. Pokud φ vychází větší než $\pi/2$, vezmeme místo něj úhel $\pi - \varphi$ stejně, jako jsme to dělali při zjišťování úhlu mezi přímkami. Platí:

$$\sin\alpha = \cos(\pi/2 - \alpha) = \cos\varphi = \frac{|\boldsymbol{u} \cdot \boldsymbol{n}|}{\|\boldsymbol{u}\|\,\|\boldsymbol{n}\|}, \quad \text{tj.} \quad \alpha = \arcsin\frac{|\boldsymbol{u} \cdot \boldsymbol{n}|}{\|\boldsymbol{u}\|\,\|\boldsymbol{n}\|}\,. \tag{9.7}$$

9.60. Příklad. Vyšetříme vzájemnou polohu přímky $p = (1, 2, 3) + \langle(1, 0, 2)\rangle$ a roviny ϱ, která prochází bodem $B = (3, 3, 1)$ a má normálový vektor $\boldsymbol{n} = (2, 1, 0)$. Souřadnice jsou dány v kartézském souřadnicovém systému.

Na základě skutečnosti, že $B \in \varrho$, můžeme doplnit konstantu d do rovnice roviny, kterou zatím máme ve tvaru $2x + y + 0z + d = 0$. Dosazením souřadnic bodu B máme $2 \cdot 3 + 3 + d = 0$, takže $d = -9$ a rovnice roviny ϱ je ve tvaru $2x + y - 9 = 0$.

Směrový vektor přímky $(1, 0, 2)$ není kolmý na normálový vektor roviny $(2, 1, 0)$, protože skalární součin $(1, 0, 2) \cdot (2, 1, 0) = 2$. Přímka tedy protíná rovinu. Spočítáme úhel mezi přímkou a rovinou podle vzorce (9.7):

$$\alpha = \arcsin\frac{|(1, 0, 2) \cdot (2, 1, 0)|}{\|(1, 0, 2)\|\,\|(2, 1, 0)\|} = \arcsin\frac{2}{\sqrt{5}\sqrt{5}} = \arcsin\frac{2}{5}\,.$$

Nyní spočítáme průsečík přímky p s rovinou ϱ. Do rovnice roviny dosadíme parametrické rovnice přímky $x = 1 + t$, $y = 2$, $z = 3 + 2t$:

$$2 \cdot (1 + t) + 2 - 9 = 0, \quad \text{tj.} \quad 2t - 5 = 0, \quad \text{tj.} \quad t = \frac{5}{2}\,.$$

Průsečík má souřadnice $P = (1, 2, 3) + \frac{5}{2}(1, 0, 2) = (\frac{7}{2}, 2, 8)$.

9.61. Příklad. Vyšetříme vzájemnou polohu dvou rovin. Nechť rovina ϱ prochází bodem A a má normálový vektor $\boldsymbol{m}$ a rovina σ prochází bodem B a má normálový vektor $\boldsymbol{n}$.

Vzájemná poloha dvou rovin

Pokud jsou vektory $\boldsymbol{m}$ a $\boldsymbol{n}$ lineárně nezávislé, roviny se protínají v přímce p. Tuto průsečnici najdeme jako množinu všech řešení soustavy dvou lineárních rovnic rovin ϱ a σ o třech neznámých x, y, z. Nebo můžeme vypočítat směrový vektor průsečnice jako vektorový součin $\boldsymbol{u} = \boldsymbol{m} \times \boldsymbol{n}$, protože průsečnice musí být kolmá k oběma normálovým vektorům. I v tomto případě ale musíme najít ještě aspoň partikulární řešení zmíněné soustavy dvou lineárních rovnic, abychom mohli průsečnici popsat ve tvaru $p = P + \langle \boldsymbol{u} \rangle$.

Pokud jsou vektory $\boldsymbol{m}$ a $\boldsymbol{n}$ lineárně závislé, roviny jsou rovnoběžné nebo splývají. Druhý případ poznáme tak, že je $B \in \varrho$. Vzdálenost rovnoběžných rovin ϱ a σ vypočítáme jako vzdálenost bodu $B \in \sigma$ od roviny ϱ, viz příklad 9.58.

Úhel mezi dvěma různoběžnými rovinami ϱ a σ je shodný s úhlem φ mezi vektory $\boldsymbol{m}$ a $\boldsymbol{n}$ až na to, že pokud vychází tento úhel větší než $\pi/2$, bereme místo něj hodnotu $\pi - \varphi$ (podobně jako při měření úhlu mezi přímkami). Dostáváme tedy vzorec:

$$\varphi = \arccos\frac{|\boldsymbol{m} \cdot \boldsymbol{n}|}{\|\boldsymbol{m}\|\,\|\boldsymbol{n}\|}\,. \tag{9.8}$$

9.62. Příklad. Jsou dány roviny ϱ a σ svými rovnicemi v kartézských souřadnicích:

$$\begin{aligned} \varrho:& \qquad x + y + 2z - 1 = 0,\\ \sigma:& \qquad x - y \qquad\;\; + 1 = 0. \end{aligned} \tag{9.9}$$

Vyšetříme jejich vzájemnou polohu.

Normálový vektor roviny ϱ je $(1,1,2)$ a normálový vektor roviny σ je $(1,-1,0)$. Tyto dva vektory jsou lineárně nezávislé, takže se roviny protínají. Množina všech řešení soustavy (9.9) je

$$p = (0,1,0) + \langle(-1,-1,1)\rangle,$$

což je průsečnice rovin ϱ a σ. Úhel mezi rovinami je

$$\varphi = \arccos \frac{|(1,1,2)\cdot(1,-1,0)|}{\|(1,1,2)\|\;\|(1,-1,0)\|} = \arccos 0 = \frac{\pi}{2},$$

takže roviny jsou na sebe kolmé.

9.63. Příklad. Jsou dány roviny ϱ a σ svými rovnicemi v kartézských souřadnicích:

$$\begin{aligned} \varrho: &\qquad x + y - 2z - 1 = 0 \\ \sigma: &\qquad -x - y + 2z + 3 = 0 \end{aligned} \tag{9.10}$$

Vyšetříme jejich vzájemnou polohu.

Normálový vektor roviny ϱ je $(1,1,-2)$ a normálový vektor roviny σ je $(-1,-1,2)$. Tyto dva vektory jsou lineárně závislé, takže roviny ϱ a σ jsou rovnoběžné. Protože soustava (9.10) nemá žádné řešení, roviny nesplývají.

Najdeme si nějaké body $A \in \varrho$, $B \in \sigma$. Při $y = 0$, $z = 0$ vychází pro rovinu ϱ souřadnice $x = 1$ a pro rovinu σ vychází $x = 3$. Máme tedy $A = (1,0,0)$, $B = (3,0,0)$. Vzdálenost dvou rovnoběžných rovin spočítáme jako vzdálenost bodu B od roviny ϱ podle vzorce (9.6):

$$v = \frac{|(B-A)\cdot \boldsymbol{n}|}{\|\boldsymbol{n}\|} = \frac{|(2,0,0)\cdot(1,1,-2)|}{\|(1,1,-2)\|} = \frac{2}{\sqrt{1^2+1^2+2^2}} = \frac{2}{\sqrt{6}}\,.$$

9.64. Příklad. Najdeme bod Q', který je souměrný s bodem Q podle roviny ϱ. Nechť má tato rovina v kartézských souřadnicích rovnici $x - 2y + z - 1 = 0$ a nechť je $Q = (-1,5,0)$. *Souměrné body*

Body Q a Q' leží na společné kolmici k k rovině ϱ, jsou stejně vzdáleny od roviny a leží v opačných částech prostoru $\mathbf{E}_3$, které rovina ϱ ohraničuje.

Směrový vektor kolmice k je roven normálovému vektoru roviny ϱ, takže je

$$k = (-1,5,0) + \langle(1,-2,1)\rangle.$$

Dosadíme hodnoty x, y, z z parametrických rovnic kolmice do rovnice roviny:

$$x = -1 + t, \quad y = 5 - 2t, \quad z = t, \quad (-1+t) - 2\,(5-2t) + t - 1 = -12 + 6t = 0, \quad \text{tj.} \quad t = 2.$$

Pokud pro $t = 2$ získáme průsečík kolmice s rovinou, pak pro dvojnásobnou hodnotu parametru $t = 4$ dostaneme hledaný bod Q'. Je tedy $Q' = (-1,5,0) + 4\,(1,-2,1) = (3,-3,4)$.

9.65. Příklad. Najdeme bod Q', který je souměrně sdružený podle přímky $p = A + \langle \boldsymbol{u} \rangle$ s bodem Q.

Body Q a Q' leží na společné přímce k, která je kolmá na přímku p a protíná ji. Mají stejnou vzdálenost od průsečíku P a leží na opačných polopřímkách přímky k, které mají počátek v bodě P. Přímka k leží v rovině σ, která je kolmá na vektor $\boldsymbol{u}$, takže $\boldsymbol{u}$ je normálovým vektorem této roviny. Průsečík P spočítáme jako průsečík roviny σ s přímkou p a pro hledaný bod Q' platí $Q' = P + (P - Q)$.

Nechť jsou například dány kartézské souřadnice $Q = (-4,5,8)$, $A = (-6,1,1)$, $\boldsymbol{u} = (5,1,3)$. Rovnice roviny σ je $5x + y + 3z + d = 0$. Protože $Q \in \sigma$, dostáváme $d = -9$, takže rovina σ je určena rovnicí $5x + y + 3z - 9 = 0$. Spočítáme dále průsečík přímky p s rovinou σ:

$$5\,(-6+5t) + (1+t) + 3\,(1+3t) - 9 = -35 + 35t = 0, \quad \text{tj.} \quad t = 1.$$

Průsečík přímky p s rovinou σ tedy je $P = (-6,1,1) + 1\,(5,1,3) = (-1,2,4)$. Nyní spočítáme souřadnice hledaného bodu:

$$Q' = (-1,2,4) + (P - Q) = (-1,2,4) + (3,-3,-4) = (2,-1,0).$$

9.66. Příklad. Ukážeme geometrickou interpretaci množiny řešení soustavy tří lineárních rovnic o třech neznámých. *Tři roviny*

Ztotožníme-li uspořádanou trojici (x, y, z) s bodem v $\mathbf{E}_3$, pro který jsou (x, y, z) jeho souřadnice vzhledem k nějakému pevně zvolenému souřadnicovému systému, můžeme mluvit o množinách řešení soustavy jako o bodech, přímkách a rovinách. Pak jsou jednotlivé rovnice soustavy též rovnicemi rovin. Tři rovnice v soustavě znamenají, že pracujeme se třemi rovinami. Množina všech řešení takové soustavy je pak společným průnikem všech tří rovin.

Dvě rovnice jsou rovnicemi stejné roviny právě tehdy, když jedna rovnice je násobkem druhé. Pro další rozbor tento případ vyloučíme a budeme tedy pracovat se třemi rovinami, z nichž žádné dvě nejsou totožné. Označíme ještě symbolem M_0 lineární prostor řešení přidružené homogenní soustavy.

Případ $\dim M_0 = 3$ můžeme vyloučit, protože rovnice roviny nemohou mít všechny koeficienty nulové.

Má-li soustava řešení, pak nemůže $\dim M_0 = 2$, protože to by znamenalo, že všechny tři roviny jsou totožné. Takový případ jsme před chvílí rovněž vyloučili.

Má-li soustava řešení a je-li $\dim M_0 = 1$ (tj. hodnost matice soustavy je rovna 2), pak množina všech řešení tvoří přímku, která je společnou průsečnicí všech tří rovin.

Má-li soustava jediné řešení (tj. hodnost matice soustavy je rovna 3), pak toto řešení tvoří bod P, který je společným průsečíkem všech tří rovin. Každé dvě roviny mají společnou průsečnici a tyto tři průsečnice se rovněž protínají v bodě P.

Je-li množina řešení prázdná (tj. hodnost matice soustavy je 2 a rozšířené matice soustavy je 3), pak roviny jsou buď všechny tři vzájemně rovnoběžné, nebo jsou dvě roviny rovnoběžné a třetí je protíná nebo se tyto tři roviny protínají každá s každou v nějaké průsečnici a tyto tři průsečnice jsou rovnoběžné. K rozlišení těchto případů můžeme použít testy na lineární závislost a nezávislost normálových vektorů odpovídajících rovin podobně, jako v příkladě 9.61.

10. Lineární algebra v teorii kódování

10.1. Poznámka. Teorie kódování řeší otázku, jak převést danou informaci do slov, která používají znaky nějaké abecedy (obvykle abecedy jedniček a nul) pokud možno efektivně, tj. bez zbytečného zatěžování přenosových linek a paměťových médií nadbytečnými informacemi. Typickým příkladem kódování je ASCII kód, který písmenům anglické abecedy a běžným znakům přiřazuje sedmibitová slova. Navíc se při kódování často řeší otázka, jakým způsobem efektivně přidat k zakódované informaci dodatečné bity tak, aby byla informace odolná vůči šumu na přenosové lince nebo menším chybám na paměťovém médiu. Dekodér, tj. zařízení, které má za úkol restaurovat původní informaci, může být postaven za nekvalitní linkou a může tedy dostat informaci zkreslenou. Z vhodně navržených dodatečných bitů může dekodér zjistit, zda informace při průchodu linkou byla poškozena a v lepším případě dokáže chybu také opravit.

Při návrhu vhodného kódování s možností detekce a opravy chyb se už od padesátých let minulého století používala lineární algebra. Tuto kapitolu završíme příkladem konstrukce tzv. lineárních Hammingových kódů. To samozřejmě zdaleka nepokrývá veškerou problematiku teorie kódování, zájemce o další studium této problematiky může použít třeba [1].

Někteří laici možná nerozlišují slovo kódování od slova šifrování. Šifrování je převod informace do takového stavu, aby ji bylo možné zpětně zrestaurovat jen pověřenými osobami. Tuto problematiku, ačkoli matematicky rovněž velmi zajímavou a ze strategického hlediska velmi důležitou, zde řešit nebudeme.

10.2. Poznámka. Definice lineárního prostoru 1.6 předpokládá, že skaláry (čísla, kterými násobíme vektory) jsou reálná čísla. V této kapitole budeme pracovat s modifikovanou definicí lineárního prostoru, kde reálná čísla nahradíme tělesem $\mathbf{Z}_2$. *Těleso* $\mathbf{Z}_2$

Poznamenávám, že pojem tělesa jsem přesně zavedl v textu za poznámkou 1.29. Pokud čtenář tuto část textu přeskočil, může si pod pojmem těleso zhruba představit množinu s operacemi sčítání a násobení. Tyto operace mají podobné vlastnosti, jako sčítání a násobení reálných čísel (komutativita, asociativita, distributivita, atd.).

10.3. Definice. *Těleso* $\mathbf{Z}_2$ je dvoubodová množina $\{0, 1\}$, na které je definováno sčítání $+ : \mathbf{Z}_2 \times \mathbf{Z}_2 \to \mathbf{Z}_2$ a násobení $\cdot : \mathbf{Z}_2 \times \mathbf{Z}_2 \to \mathbf{Z}_2$ takto:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad\qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Tedy: $0 + 0 = 0, \quad 0 + 1 = 1 + 0 = 1, \quad 1 + 1 = 0, \quad 0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1.$

10.4. Poznámka. Sčítání na $\mathbf{Z}_2$ je shodné s logickou operací XOR (vylučovací nebo) a násobení na $\mathbf{Z}_2$ je shodné s operací AND (logická konjunkce).

Nebo jinak: Násobení na $\mathbf{Z}_2$ je stejné, jako jsme zvyklí násobit celá čísla, a sčítání skoro taky, až na jedinou výjimku: $1 + 1 = 0$.

Nebo ještě jinak: Prvek 0 v $\mathbf{Z}_2$ si můžeme představit jako jakékoli sudé číslo a prvek 1 jako jakékoli číslo liché. Sčítáme a násobíme pak sudá čísla se sudými, s lichými atd. Tyto operace pak dávají jako výsledek čísla sudá nebo lichá přesně podle pravidel počítání v $\mathbf{Z}_2$.

Nebo ještě jinak: provedeme operaci sčítání a násobení jako v případě celých čísel, ale pokud výsledek padne mimo množinu $\{0, 1\}$, použijeme zbytek při dělení výsledku číslem 2.

10.5. Příklad. Na množině uspořádaných n-tic prvků ze $\mathbf{Z}_2$, tj. na množině $\mathbf{Z}_2^n$, zavedeme operaci sčítání $+ : \mathbf{Z}_2^n \times \mathbf{Z}_2^n \to \mathbf{Z}_2^n$ analogicky, jako v případě sčítání uspořádaných n-tic reálných čísel, jen samozřejmě pracujeme se sčítáním podle definice 10.3. Pro $(a_1, \ldots, a_n) \in \mathbf{Z}_2^n$ a $(b_1, \ldots, b_n) \in \mathbf{Z}_2^n$ definujeme

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

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 nulou přirozeným způsobem:

$$1 \cdot (a_1, \ldots, a_n) \stackrel{\text{df}}{=} (a_1, \ldots, a_n), \qquad 0 \cdot (a_1, \ldots, a_n) \stackrel{\text{df}}{=} (0, \ldots, 0).$$

Povšimněte si analogie s příklady 1.11 a 1.69.

Pokud nahradíme v definici lineárního prostoru 1.6 množinu reálných čísel $\mathbf{R}$ nějakým tělesem, pak takovému lineárnímu prostoru říkáme, že je definován „nad tělesem“ (podrobněji viz definici 1.67). V tomto příkladě jsme zavedli na množině $\mathbf{Z}_2^n$ operace tak, že dostáváme *lineární prostor nad tělesem* $\mathbf{Z}_2$.

Nulový vektor tohoto lineárního prostoru je vektor $(0, \ldots, 0)$. Tento lineární prostor má celkem 2^n vektorů, které mezi sebou umíme sčítat a samozřejmě tyto vektory umíme násobit jedničkou nebo nulou.

10.6. Poznámka. Na rozdíl od lineárních prostorů nad $\mathbf{R}$ náš nově zavedený lineární prostor nad $\mathbf{Z}_2$ má konečně mnoho prvků. To je jediný rozdíl vzhledem k lineárním prostorům, které jsme dosud studovali. Všechny ostatní vlastnosti zůstávají stejné. *Počítání v* $\mathbf{Z}_2$

10.7. Poznámka. Každý vektor z $\mathbf{Z}_2^n$ je sám sobě opačným vektorem, tj. $\forall \boldsymbol{x} \in \mathbf{Z}_2^n : \boldsymbol{x} = -\boldsymbol{x}$, neboli $\boldsymbol{x} + \boldsymbol{x} = \boldsymbol{o}$. Díky tomu v tělese $\mathbf{Z}_2$ a v lineárním prostoru nad tímto tělesem nemusíme rozlišovat mezi sčítáním a odčítáním.

10.8. Příklad. Najdeme dimenzi a bázi lineárního obalu čtyř vektorů v $\mathbf{Z}_2^5$:

$$M = \langle (1,0,1,0,1), (1,1,0,0,1), (1,0,0,1,1), (0,1,1,0,0) \rangle.$$

Řešení: Protože Gaussova eliminace nemění lineární obal, najdeme bázi eliminací:

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

Báze M je tedy například $(1,0,1,0,1), (0,1,1,0,0), (0,0,1,1,0)$. Dimenze M je tři.

10.9. Poznámka. Protože $\mathbf{Z}_2^n$ obsahuje konečný počet vektorů, můžeme (na rozdíl od lineárních prostorů nad $\mathbf{R}$) vypsat podprostor nebo lineární obal výčtem prvků. Pro podprostor M z předchozího příkladu platí:

$$\begin{aligned} M = \{&(0,0,0,0,0), (1,0,1,0,1), (0,1,1,0,0), (0,0,1,1,0),\\ &(1,1,0,0,1), (1,0,0,1,1), (0,1,0,1,0), (1,1,1,1,1)\}. \end{aligned}$$

Jak se dá takový výčet prvků najít? Především pro $\boldsymbol{x} \neq \boldsymbol{o}$ je $\langle \boldsymbol{x} \rangle = \{\boldsymbol{o}, \boldsymbol{x}\}$. Skutečně, vektor $\boldsymbol{x}$ můžeme násobit jen jedničkou nebo nulou. To jsou všechny lineární kombinace, které můžeme s vektorem $\boldsymbol{x}$ vytvořit. Množina M má tříprvkovou bázi $\{\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}\}$. Takže pro sestavení lineárního obalu stačí najít všechny lineární kombinace těchto tří vektorů: $\boldsymbol{o}$, $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, $\boldsymbol{a}+\boldsymbol{b}$, $\boldsymbol{a}+\boldsymbol{c}$, $\boldsymbol{b}+\boldsymbol{c}$, $\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{c}$.

10.10. Příklad. Zjistěte počet prvků lineárního (pod)prostoru nad $\mathbf{Z}_2$, který má dimenzi n.

Řešení: Má-li (pod)prostor dimenzi n, pak má n prvkovou bázi $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n$. Abychom získali všechny lineární kombinace těchto vektorů, musíme každý vektor násobit jedničkou nebo nulou. Máme tedy 2^n lineárních kombinací. Tyto kombinace vyplňují celý lineární (pod)prostor a jsou navzájem různé. Kdyby se totiž dvě lineární kombinace s různými koeficienty rovnaly, pak jejich odečtením dostáváme netriviální lineární kombinaci rovnu nulovému vektoru. To je spor se skutečností, že $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n$ je báze.

Závěr: počet prvků lineárního (pod)prostoru nad $\mathbf{Z}_2$ dimenze n je 2^n. Například podprostor M z příkladu 10.8 má dimenzi 3 a má tedy $2^3 = 8$ prvků.

10.11. Příklad. Najděte všechna řešení $\boldsymbol{x} \in \mathbf{Z}_2^6$ homogenní soustavy rovnic $\mathbf{A}\,\boldsymbol{x} = \boldsymbol{o}$, je-li

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

Řešení: Najdeme matici ekvivalentní soustavy s lineárně nezávislými řádky:

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

Hodnost matice soustavy je 4, dimenze prostoru je 6, takže dimenze množiny řešení je 2. Hledáme tedy dvě lineárně nezávislá řešení: $(?,?,?,?,1,0)$ a $(?,?,?,?,0,1)$. Dosazením „zespoda nahoru“ dostáváme následující řešení: $(0,1,1,1,1,0)$, $(0,1,0,0,0,1)$.

Množina všech řešení je lineárním obalem těchto dvou řešení a obsahuje $2^2 = 4$ vektory:

$$\langle (0,1,1,1,1,0), (0,1,0,0,0,1) \rangle = \{(0,0,0,0,0,0), (0,1,1,1,1,0), (0,1,0,0,0,1), (0,0,1,1,1,1)\}.$$

10.12. Poznámka. Při hledání báze prostoru řešení můžeme také využít větu 5.34. V předchozím příkladě bychom pak pokračovali v eliminaci zpětným chodem:

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

Tvar matice $(\mathbf{E}|\mathbf{C})$ odpovídá předpokladu věty 5.34, takže řádky báze řešení tvoří matici:

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

Poznamenejme, že nemusíme přecházet od matice $\mathbf{C}$ k matici $-\mathbf{C}$, protože v aritmetice $\mathbf{Z}_2$ jsou obě matice stejné.

10.13. Definice. Nechť A je konečná množina (tzv. *abeceda*). Pak *slovo* je libovolná konečná posloupnost prvků z A.

Kód, kódové slovo

Kódování v obecném smyslu zahrnuje (1) algoritmus, kterým informace převádíme do posloupnosti slov (tzv. *kodér*) a (2) algoritmus, kterým zpětně z těchto slov získáváme původní informaci (*dekodér*).

Slova, která vytváří kodér, se nazývají *kódová slova*. Množina všech kódových slov se nazývá *kód*.

Je-li kód množinou slov stejné délky (každé kódové slovo má stejný počet znaků abecedy), mluvíme o tzv. *blokovém kódu*. Blokový kód *délky n* značí, že všechna kódová slova mají n znaků abecedy.

10.14. Poznámka. Typicky $A = \{0, 1\}$, tj. abeceda se skládá jen ze dvou znaků (tzv. bitů, anglicky bits, což je původně zkratka z BInary digiTS) a slova jsou posloupnosti těchto bitů.

10.15. Příklad. ASCII kód je množina 7bitových slov, která reprezentují jednotlivá písmena anglické abecedy a další běžné znaky (číslice, tečku, vykřičník, otazník, mezeru, # neboli vězení atd.). Tato množina obsahuje 91 slov, protože v době vzniku tohoto kódu byl požadavek na kódování 91 znaků. Kodér i dekodér pak pracují s tabulkou těchto znaků, u kterých jsou uvedena odpovídající kódová slova. Tato tabulka může být na straně kodéru technicky realizována třeba ovladačem klávesnice a na straně dekodéru fontem.

Jedná se o blokový kód. Od počátku existence počítačů byl tento blokový kód rozšířen o redundantní nulový bit na začátku, takže často je ASCII kód prezentován jako množina 8bitových slov. Později začal být tento bit využíván pro různá rozšíření ASCII kódu, která zahrnují i reprezentaci některých písmen s diakritickými znaménky.

10.16. Poznámka. Je potřeba si uvědomit, že slova jsou do paměťového média nebo do přenosové linky vkládána za sebou bez oddělovačů. Blokový kód má tu výhodu, že dekodér dokáže snadno rozdělit tento „tok znaků abecedy“ na slova a těm pak přidělit význam například pomocí nějaké tabulky. Nevýhoda blokového kódu spočívá v tom, že plýtvá místem, neboť tušíme, že pokud navrhneme pro častěji se vyskytující slova kratší posloupnosti znaků, celkový počet znaků abecedy pro přenášené/ukládané informace může být menší. To ostatně je (alespoň zhruba) i vlastnost přirozeného jazyka. Tam máme ovšem abecedu rozsáhlejší (nebinární) a za prvek abecedy můžeme považovat i mezeru: oddělovač mezi slovy, který dekodéru pomůže. Nebo v Morseově abecedě máme také tři znaky: tečka, čárka a mezera. Bez mezery by bylo dekódování morseovky nemožné. Máme-li k dispozici jen binární abecedu $A = \{0, 1\}$, pak je potřeba při návrhu kódu se slovy nestejné délky myslet na možnosti dekodéru. Je to technicky možné, ale není to obsahem tohoto textu. Příkladem neblokového kódu je UTF8, který kóduje znaky abeced všech jazyků světa. Písmena anglické abecedy a běžné znaky jsou reprezentovány 8bitovým slovem, ale písmena dalších jazyků jsou kódována 16bitovým slovem nebo i delším (24 bitů a 32 bitů).

Nadále budeme pracovat jen s blokovými kódy nad binární abecedou.

10.17. Poznámka. Nechť K je blokový kód délky n nad binární abecedou A. Pak platí $K \subseteq A^n$.

Kódování s detekcí a opravou chyb

Pokud $K \neq A^n$, pak mezi uspořádanými n-ticemi z A existují nekódová slova, tj. taková, která kodér nikdy nevytvoří a která nemají přidělen význam. Přijme-li dekodér (např. za nekvalitní linkou) nekódové slovo, je si jist, že při přenosu linkou došlo k chybě. Může například v takovém případě požádat pomocí jiných technických prostředků kodér, aby vyslal slovo znovu. Nebo se může pokusit chybu opravit.

Tušíme jisté problémy: šum na lince může způsobit tak nešťasnou chybu, že se z jednoho kódového slova stane jiné kódové slovo a dekodér nic nepozná. Je tedy rozumné kódování navrhnout tak, aby například omezený počet chyb v jednom slově (tj. záměn nuly za jedničku a naopak) zaručil, že se z kódového slova stane slovo nekódové.

Znovu můžeme hledat analogii v přirozeném jazyce. Překlep ve slově jsme velmi často schopni detekovat i opravit. Někdy ale překlep může způsobit, že vzniká jiné běžné slovo jazyka. Člověk jako dekodér ani s tímto druhem chyby nemá většinou problém, protože pracuje s kontextem celé věty (větší skupiny slov). Takto inteligentní dekodér ale nebude naším cílem. Vystačíme si s detekováním a opravováním chyb jen na úrovni jednotlivých slov.

10.18. Definice. Nechť $A = \{0, 1\}$. *Hammingova velikost slova* $\boldsymbol{u} \in A^n$ je počet jedniček v tomto slově a značíme ji $\|\boldsymbol{u}\|$. *Hammingova vzdálenost slov* $\boldsymbol{v} \in A^n$ *a* $\boldsymbol{w} \in A^n$ je počet bitů, ve kterých se tato dvě slova liší. Značíme ji $\mathrm{d}(\boldsymbol{v}, \boldsymbol{w})$.

10.19. Poznámka. Nechť $A = \{0, 1\}$ a $\boldsymbol{v}, \boldsymbol{w} \in A^n$. Pak $\boldsymbol{v} + \boldsymbol{w}$ (v aritmetice $\mathbf{Z}_2$) je slovo, které má jedničky právě v místech, kde se $\boldsymbol{v}$ a $\boldsymbol{w}$ liší. Takže platí: $\mathrm{d}(\boldsymbol{v}, \boldsymbol{w}) = \|\boldsymbol{v} + \boldsymbol{w}\|$.

10.20. Poznámka. Předpokládejme, že $\boldsymbol{v}$ je slovo vyslané kodérem a $\boldsymbol{w}$ slovo přijaté dekodérem. Pak $\mathrm{d}(\boldsymbol{v}, \boldsymbol{w})$ udává počet chyb ve slově, které vznikly během přenosu.

Poznámka v poznámce: předpokládáme, že díky technickým parametrům zařízení nikdy nedojde k chybě, kdy se jednička nebo nula ze slova zcela vytratí nebo vznikne nová, tj. nikdy nehrozí riziko, že by na straně dekodéru byl přečten jiný počet jedniček a nul než byl vyslán kodérem.

10.21. Příklad. Je dán tento kód: $K = \{0000, 0011, 0101, 1001, 0110, 1010, 1100, 1111\}$. Jedná se o blokový binární kód délky 4. Pro potřeby tohoto příkladu nebudeme specifikovat druh informace, kterou potřebujeme přenášet. Protože kód obsahuje jen 8 slov, může být původní informace zapsána pomocí nějaké 8 znakové abecedy.

Zajímavé na tomto kódu je, že každé kódové slovo obsahuje sudý počet jedniček. Pokud dojde k jediné chybě ve slovu, máme jistotu, že dekodér přijme nekódové slovo (s lichým počtem jedniček) a ohlásí chybu. Je-li pravděpodobnost výskytu dvou nebo více chyb v jednom slově zanedbatelná a nám postačuje jen detekovat chyby (neopravovat je), je toto rozumný návrh kódu.

Povšimneme si, že minimální Hammingova vzdálenost mezi dvěma různými kódovými slovy tohoto kódu je 2, takže jedna chyba způsobí vytvoření nekódového slova.

10.22. Příklad. Je dán blokový kód délky 8 bitů: $K = \{00000000, 00001111, 11110000, 11111111\}$. Minimální Hammingova vzdálenost mezi kódovými slovy je 4, takže ani tři chyby ve slově nezpůsobí přechod na jiné kódové slovo a dekodér správně detekuje chybu přenosu. Dekodér dokonce dokáže v tomto kódu opravit jednu chybu a detekovat výskyt dvou chyb ve slově. Chybu opraví tak, že se od přijatého slova $\boldsymbol{w}$ vrátí ke kódovému slovu $\boldsymbol{v}$ takovému, že Hammingova vzdálenost $\mathrm{d}(\boldsymbol{v}, \boldsymbol{w}) = 1$. Samozřejmě, naučíme-li dekodér opravovat jednu chybu ve slově, pak už nemusí být schopen vždy správně detekovat tři chyby. Může se totiž stát, že místo toho opraví jeden bit a dostane jiné kódové slovo.

10.23. Příklad. Nechť minimální Hammingova vzdálenost mezi kódovými slovy je $d > 2$. Rozhodněte (A) kolik chyb ve slově může dekodér detekovat, pokud po něm nechceme, aby chyby opravoval, a (B) kolik chyb ve slově může opravit a kolik jich může aspoň detekovat bez opravy.

Odpověď: (A) Dekodér může spolehlivě detekovat nejvýše $d-1$ chyb. (B) Je-li d sudé, může dekodér opravit jednu až $d/2 - 1$ chyb a detekovat $d/2$ chyb bez opravy. Je-li d liché, může opravit jednu až $(d-1)/2$ chyb a žádné množství chyb nedetekuje bez opravy. Je samozřejmě možné i jiné rozvržení. Např. pro d liché necháme dekodér opravit nejvýše $(d-3)/2$ chyb a při výskytu $(d-1)/2$ nebo $(d+1)/2$ chyb ve slově jen chyby detekujeme bez opravy.

10.24. Poznámka. Při návrhu dekodéru s detekcí nebo opravou chyb se s výhodou využijí nástroje lineární algebry, jako je násobení matic, vymezení podprostorů a bází, řešení homogenních soustav atd. Binární slova délky n budeme v tomto případě považovat za vektory z lineárního prostoru $\mathbf{Z}_2^n$, takže je můžeme sčítat. Ostatně, už v poznámce 10.19 jsem zmínil sčítání slov $\boldsymbol{v}$ a $\boldsymbol{w}$. V teorii kódování se binární slova zapisují jedničkami a nulami bez mezer (viz příklady 10.21 a 10.22), zatímco v lineární algebře jsme dosud zapisovali vektory do závorek a jejich složky oddělovali čárkami. Věřím, že nedojde k nedorozumění, pokud dále v textu o kódování budu zapisovat vektory způsobem, jako v příkladu 10.21. *Lineární kód*

10.25. Definice. Binární blokový kód K délky n je *lineární*, pokud K tvoří lineární podprostor lineárního prostoru $\mathbf{Z}_2^n$. Jestliže dimenzi tohoto podprostoru označíme k, pak mluvíme o *lineárním* (n,k) *kódu.*

10.26. Věta. Nejmenší Hammingova vzdálenost mezi slovy lineárního kódu K je rovna nejmenší Hammingově velikosti nenulového kódového slova.

Důkaz. Stačí si uvědomit, že pro $\boldsymbol{v}_1, \boldsymbol{v}_2 \in K$ je $\|\boldsymbol{v}_1 + \boldsymbol{v}_2\| = \mathrm{d}(\boldsymbol{v}_1, \boldsymbol{v}_2)$, a přitom $\boldsymbol{v}_1 + \boldsymbol{v}_2 \in K$, protože K je lineární kód. Navíc $\|\boldsymbol{v}\| = \mathrm{d}(\boldsymbol{v}, \boldsymbol{o})$.

10.27. Příklad. Kód z příkladu 10.21 je lineární, protože K tvoří podprostor lineárního prostoru $\mathbf{Z}_2^4$. Skutečně, sečteme-li dva vektory se sudým počtem jedniček, dostameme vektor se sudým počtem jedniček. Výsledek násobení vektoru z K konstantou α zůstane v K, protože v $\mathbf{Z}_2$ číslo α může být jen 0 nebo 1.

Báze kódu z příkladu 10.21 je například $\{0011, 0101, 1100\}$, takže dimenze kódu je 3 a jedná se tedy o *lineární* $(4,3)$ *kód.*

10.28. Poznámka. Příklad 10.21 ilustruje tzv. kódování s kontrolním bitem parity. Původní informaci s osmi znaky je možné kódovat blokovým binárním kódem $\{000, 001, 010, 011, 100, 101, 110, 111\}$, tedy stačí nám tři bity. Pokud chceme detekovat jednu chybu ve slově, přidáme čtvrtý tzv. *kontrolní bit*, který nastavíme na 0, pokud je v původním tříbitovém slově sudý počet jedniček a nastavíme ho na 1, pokud je v původním slově lichý počet jedniček. Dostáváme tak kód z příkladu 10.21.

Tento postup můžeme použít na jakýkoli „výchozí“ binární blokový kód délky k se všemi 2^k kódovými slovy. Přidáním kontrolního bitu parity dostáváme lineární $(k+1,k)$ kód, kterým jsme schopni detekovat jednu chybu ve slově. Dekodér pak odstraní kontrolní bit z každého přijatého slova a získá tím původní kódovanou informaci.

10.29. Poznámka. Vstupní informace je často připravena už jako posloupnost slov binárního blokového kódu délky k, ve kterém všechna slova jsou kódová. Naším úkolem je pak rozšířit tento kód o dalších $n-k$ tzv. *kontrolních bitů*, abychom dostali lineární (n,k) kód. Kodér tedy očekává na vstupu libovolné slovo délky k a jeho úkolem je zkopírovat bity vstupu do výstupu (tzv. *informační bity*) a přidat $n-k$ kontrolních bitů. Dekodér pak použije tyto kontrolní bity pro detekci a případnou opravu chyb a poté je odstraní a ponechá jen informační bity. Cílem je navrhnout kódování, které má co nejmenší *redundanci* (tj. poměr počtu kontrolních bitů ku počtu všech přenášených bitů ve slově), protože ta zatěžuje linku nebo paměťové médium režijními informacemi, které uživatel ze svého pohledu nevyužije. Přitom ale chceme co nejschopnější dekodér, který by detekoval a opravoval chyby a navíc by měl pracovat efektivně.

Z pohledu lineární algebry je výše popsaný přechod od kódu délky k na lineární kód délky $n > k$ lineární zobrazení $\mathcal{A}\colon \mathbf{Z}_2^k \to \mathbf{Z}_2^n$, které je prosté (jinak by docházelo ke ztrátě informace). Podle věty 7.20 množina obrazů tohoto zobrazení (neboli kód) tvoří lineární podporostor v $\mathbf{Z}_2^n$. Bázi tohoto podprostoru můžeme hledat tak, že sepíšeme bázi ve výchozím prostoru $\mathbf{Z}_2^k$ a najdeme její obraz za použití zobrazení $\mathcal{A}$. Tento obraz podle věty 7.27 jednoznačně určuje zobrazení $\mathcal{A}$ na celém $\mathbf{Z}_2^k$.

Kodérem je přímo zobrazení $\mathcal{A}$ a možným dekodérem je zobrazení inverzní k $\mathcal{A}$ definované na $\mathcal{A}(Z_2^k)$. Ovšem dekodér se musí umět vyrovnat i se slovy, která jsou nekódová, tj. neleží v množině $\mathcal{A}(Z_2^k)$. To inverzní zobrazení k $\mathcal{A}$ neumí.

10.30. Příklad. Nechť je vstupní informace kódována binárním blokovým kódem délky k se všemi 2^k slovy. Kodér této informace navrhneme tak, že každé vstupní slovo zopakuje a vytvoří výstupní slovo délky $2k$. Tím vzniká lineární $(2k,k)$ kód. Minimální Hammingova vzdálenost mezi dvěma kódovými slovy je 2, takže dekodér spolehlivě detekuje jednu chybu ve slově. Za jistých okolností může detekovat i více chyb ve slově, pokud chyba v první polovině slova se nezopakuje na stejném bitu druhé poloviny slova. V žádném případě ale dekodér nemůže odhalenou chybu spolehlivě opravit. Redundance je příliš vysoká, a přitom neumíme ani opravit chyby. Asi to nebude nejlepší možný návrh kódování.

10.31. Příklad. Kód z příkladu 10.22 je lineární. Nevýhoda tohoto kódu ale spočívá v tom, že kódová slova mohou reprezentovat jen čtyři rozdílné stavy původní informace, ale mají příliš mnoho bitů, které zbytečně zatěžují paměťové médium nebo přenosové linky. Proto se Hamming zaměřil na hledání jiných vhodnějších lineárních kódů.

10.32. Definice. *Generující matice lineárního kódu K* je po řádcích zapsaná báze tohoto kódu. *Kontrolní matice lineárního kódu K* je taková matice $\mathbf{H}$ s lineárně nezávislými řádky, pro kterou platí: množina řešení homogenní soustavy $\mathbf{H}\,\boldsymbol{x} = \boldsymbol{o}$ je rovna kódu K.

Generující a kontrolní matice

10.33. Věta. Nechť $\mathbf{G}$ je generující matice a $\mathbf{H}$ kontrolní matice lineárního (n, k) kódu. Pak $\mathbf{G}$ má k řádků a $\mathbf{H}$ má $n - k$ řádků. Obě matice mají n sloupců. Jinými slovy, generující matice má tolik řádků, kolik je v kódu informačních bitů, kontrolní matice má tolik řádků, kolik má kód kontrolních bitů a počet sloupců obou matic je roven počtu přenášených bitů v jednom slově.

Důkaz. Matice $\mathbf{G}$ má k řádků, protože báze prostoru dimenze k obsahuje k vektorů. Počet řádků matice H plyne z věty 5.14. Konečně n sloupců obou matic plyne přímo z definice těchto matic.

10.34. Příklad. Kód z příkladu 10.21 může mít následující generující matici:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

protože $\{1001, 0101, 0011\}$ je báze kódu K. Popíšu, jak se obvykle tato báze sestavuje. Vyjde se ze standardní báze vstupního kódu: $\{100, 010, 001\}$ a aplikuje se na ní zobrazení kodéru. Všechny tři prvky této báze mají lichý počet jedniček, takže poslední kontrolní bit kodér nastaví na jedničku.

Kontrolní matice našeho kódu je

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix},$$

protože množina řešení rovnice $x_1 + x_2 + x_3 + x_4 = 0$ je shodná s množinou slov, které mají sudý počet jedniček (sčítáme jedničky modulo 2), a to jsou právě všechna kódová slova.

10.35. Příklad. Kódujme vstupní informaci v blokovém kódu délky 4 podle příkladu 10.30 (zdvojení slova). Dostáváme lineární (8,4) kód. Jeho generující matice je

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

K vytvoření této báze jsem použil stejný postup, jako v předchozím příkladě. Na standardní bázi prostoru $\mathbf{Z}_2^4$ jsem aplikoval zobrazení kodéru. Kontrolní matice je výjimečně v tomto příkladě $\mathbf{H} = \mathbf{G}$, protože soustava rovnic

$$\begin{aligned} x_1 + x_5 &= 0 \\ x_2 + x_6 &= 0 \\ x_3 + x_7 &= 0 \\ x_4 + x_8 &= 0 \end{aligned}$$

má za řešení právě taková slova, pro která první bit je roven pátému, druhý šestému, třetí sedmému a čtvrtý osmému, tj. obě části slova se rovnají a jedná se o kódové slovo.

10.36. Poznámka. Generující matice sama o sobě jednoznačně určuje lineární kód. Kontrolní matice sama o sobě také jednoznačně určuje lineární kód. Tyto dvě matice jsou v následujícím „duálním“ vztahu:

10.37. Věta. Nechť $\mathbf{G}$ je generující a $\mathbf{H}$ je kontrolní matice lineárního (n, k) kódu. Pak $\mathbf{H} \cdot \mathbf{G}^T = \mathbf{O}_1$ a také $\mathbf{G} \cdot \mathbf{H}^T = \mathbf{O}_2$, kde $\mathbf{O}_1$ je nulová matice s $n - k$ řádky a k sloupci a $\mathbf{O}_2 = \mathbf{O}_1^T$.

Důkaz. Kód s uvedenými maticemi označíme písmenem K. Řádky matice $\mathbf{G}$ alias sloupce matice $\mathbf{G}^T$ jsou podle definice generující matice prvky kódu K. Podle definice kontrolní matice musí tyto sloupce matice $\mathbf{G}^T$ alias prvky kódu K být řešením soustavy $\mathbf{H}\,\boldsymbol{x} = \boldsymbol{o}$. Přesně to říká vztah $\mathbf{H} \cdot \mathbf{G}^T = \mathbf{O}_1$, pokud jej rozepíšeme po jednotlivých sloupcích matice $\mathbf{G}^T$.

Vztah $\mathbf{G} \cdot \mathbf{H}^T = \mathbf{O}_2$ vzniká transponováním matic na levé i pravé straně vztahu $\mathbf{H} \cdot \mathbf{G}^T = \mathbf{O}_1$.

10.38. Poznámka. Předchozí věta ukazuje, že nejen řádky matice $\mathbf{G}$ řeší soustavu $\mathbf{H}\boldsymbol{x} = \boldsymbol{o}$, ale také řádky matice $\mathbf{H}$ řeší soustavu $\mathbf{G}\boldsymbol{x} = \boldsymbol{o}$. Známe-li jen jednu z těchto matic, pak druhou lze najít tak, že najdeme bázi množiny řešení odpovídající homogenní soustavy rovnic a zapíšeme ji do řádků.

Protože velmi často je generující matice vytvořena za použití standardní báze vstupního prostoru $\mathbf{Z}_2^k$ a aplikací algoritmu kodéru na tuto bázi, který kopíruje informační bity a přidává kontrolní bity na konec slova, je matice $\mathbf{G}$ často ve tvaru $\mathbf{G} = (\mathbf{E}|\mathbf{C})$, kde $\mathbf{E}$ je jednotková matice typu (k,k). Matici $\mathbf{H}$ pak můžeme snadno najít podle věty 5.34, přitom místo matice $-\mathbf{C}^T$ stačí použít matici $\mathbf{C}^T$, protože v aritmetice $\mathbf{Z}_2$ je $\mathbf{C} = -\mathbf{C}$. Dostáváme $\mathbf{H} = (\mathbf{C}^T|\mathbf{E}')$, kde $\mathbf{E}'$ je jednotková matice typu $(n-k, n-k)$.

10.39. Příklad. S využitím věty 5.34 zkusíme sestavit kontrolní matice z příkladů 10.34 a 10.35, pokud je dána jen generující matice.

Příklad 10.34. Matice $\mathbf{C}$ z rovnosti $\mathbf{G} = (\mathbf{E}|\mathbf{C})$ obsahuje sloupec jedniček. $\mathbf{C}^T$ je tedy řádek jedniček, ke kterému podle věty 5.34 vpravo připíšeme jednotkovou matici typu $(1,1)$. Dostáváme matici $\mathbf{H}$.

Příklad 10.35. Matice $\mathbf{C}$ z rovnosti $\mathbf{G} = (\mathbf{E}|\mathbf{C})$ je jednotková matice, takže $\mathbf{C}^T = \mathbf{C}$. K této jednotkové matici podle věty 5.34 připíšeme jednotkovou matici typu $(4,4)$. Dostáváme tím matici $\mathbf{H}$, která je výjimečně rovna matici $\mathbf{G}$.

10.40. Definice. Pokud existuje generující matice lineárního kódu ve tvaru $\mathbf{G} = (\mathbf{E}|\mathbf{C})$, kde $\mathbf{E}$ je jednotková matice, nazýváme takový kód *systematický*.

10.41. Poznámka. Předchozí poznámka 10.38 ukazuje, že pro systematické kódy můžeme z generující matice snadno sestavit matici kontrolní ve tvaru $\mathbf{H} = (\mathbf{C}^T|\mathbf{E}')$. Také obráceně, pokud je dána kontrolní matice ve tvaru $\mathbf{H} = (\mathbf{C}^T|\mathbf{E}')$, je možné snadno přejít k matici generující tvaru $\mathbf{G} = (\mathbf{E}|\mathbf{C})$.

10.42. Poznámka. Nechť je dána generující matice, která není tvaru $(\mathbf{E}|\mathbf{C})$. Protože generující matice obsahuje v řádcích bázi kódu, je možné eliminací této matice přejít k jiné generující matici téhož kódu. Stačí si uvědomit, že Gaussova eliminace nemění lineární obal řádků. Může se tedy stát, že po eliminaci dostaneme novou generující matici ve tvaru $\mathbf{G} = (\mathbf{E}|\mathbf{C})$ a shledáme, že kód je systematický.

Pokud ani po eliminaci generující matice nelze dosáhnout tvaru $(\mathbf{E}|\mathbf{C})$, jedná se o nesystematický kód. I v tomto případě je ovšem eliminací možné dospět k matici, která se od matice $(\mathbf{E}|\mathbf{C})$ liší jen prohozením některých sloupců. Nesystematický kód se tedy od systematického liší jen pořadím bitů v jednotlivých kódových slovech. Přechod od generující matice ke kontrolní (nebo obráceně) je u nesystematického kódu obtížnější, protože nelze přímo použít větu 5.34, ale před jejím použitím musíme prohodit sloupce generující matice, pak přejít ke kontrolní matici a u ní prohodit sloupce zpět. Podobně bychom postupovali, pokud přecházíme od kontrolní matice nesystematického kódu k matici generující.

Systematický kód získáme zaručeně v případě, kdy necháme kodér kopírovat informační bity vstupního slova do výstupu a pak přidat bity kontrolní. Pokud ale kodér informační bity „promíchá“ s bity kontrolními, pak kód nemusí být systematický.

10.43. Věta. Kód je systematický právě tehdy, když existuje kontrolní matice tohoto kódu tvaru $(\mathbf{C}^T|\mathbf{E}')$, kde $\mathbf{E}'$ je jednotková matice.

Důkaz. Tvrzení věty je důsledkem skutečnosti, že kód má generující matici tvaru $\mathbf{G} = (\mathbf{E}|\mathbf{C})$ právě tehdy, když má kontrolní matici tvaru $\mathbf{H} = (\mathbf{C}^T|\mathbf{E}')$.

10.44. Poznámka. Je-li dána kontrolní matice v jiném tvaru než $(\mathbf{C}^T|\mathbf{E}')$, pak z toho ještě neplyne, že kód není systematický. Eliminací kontrolní matice můžeme získat jinou kontrolní matici, která ovšem přísluší stejnému kódu. Stačí si uvědomit, že eliminací matice soustavy dostáváme případně matici jiné soustavy, ale se stejnou množinou řešení. Pokud tedy po eliminaci kontrolní matice získáme matici tvaru $(\mathbf{C}^T|\mathbf{E}')$, pak je kód systematický.

10.45. Věta. Nechť $\mathbf{G}$ je generující matice lineárního (n,k) kódu. Nechť dále $\mathcal{A}\colon \mathbf{Z}_2^k \to \mathbf{Z}_2^n$ je lineární zobrazení, které zobrazuje standardní bázi prostoru $\mathbf{Z}_2^k$ na řádky matice $\mathbf{G}$. Pak matice $\mathbf{G}^T$ je maticí lineárního zobrazení $\mathcal{A}$ vzhledem ke standardním bázím. *Kodér lineárního kódu*

Důkaz. Matice lineárního zobrazení obsahuje podle definice 7.43 ve sloupcích souřadnice obrazů báze vstupního prostoru vzhledem k bázi výstupního prostoru. V našem případě generující matice $\mathbf{G}$ obsahuje v řádcích souřadnice obrazů (při zobrazení $\mathcal{A}$) standardní báze $\mathbf{Z}_2^k$ vzhledem ke standardní bázi v $\mathbf{Z}_2^n$. Abychom z řádků matice dostali sloupce podle definice matice lineárního zobrazení, stačí matici $\mathbf{G}$ transponovat.

10.46. Poznámka. Zobrazení $\mathcal{A}$ z předchozí věty matematicky popisuje kodér lineárního kódu. Jeho generující matice je $\mathbf{G}$. Věta říká, že $\mathbf{G}^T$ je matice zobrazení tohoto kodéru vzhledem ke standardním bázím. Vstupuje-li vektor $\boldsymbol{u} \in \mathbf{Z}_2^k$ do kodéru, pak jeho výstupem je vektor $\boldsymbol{v} \in \mathbf{Z}_2^n$, který spočítáme podle věty 7.49 jako součin matice zobrazení a vstupního vektoru:

$$\boldsymbol{v}^T = \mathbf{G}^T \cdot \boldsymbol{u}^T, \qquad \text{neboli:} \quad \boldsymbol{v} = \boldsymbol{u} \cdot \mathbf{G}.$$

10.47. Poznámka. Pokud kodér kopíruje k vstupních bitů do výstupu a pak přidá kontrolní bity, nemusíme prvních k bitů výstupu počítat maticovým násobením. Stačí tímto násobením počítat kontrolní bity. Generující matice má v tomto případě tvar $\mathbf{G} = (\mathbf{E}|\mathbf{C})$. Označíme-li $\boldsymbol{u}$ slovo, které vstupuje do kodéru a $\boldsymbol{v}'$ vektor, který obsahuje jen kontrolní bity výstupního slova, pak platí:

$$\boldsymbol{v}' = \boldsymbol{u} \cdot \mathbf{C}.$$

10.48. Poznámka. Dekodér při kontrole, zda se jedná o kódové slovo, použije kontrolní matici. Nechť dekodér přijme slovo $\boldsymbol{w}$. Pak $\mathbf{H} \cdot \boldsymbol{w}^T$ je nulový vektor právě tehdy, když je slovo $\boldsymbol{w}$ kódové. V takovém případě dekodér předpokládá, že nedošlo při přenosu slova k chybě, odstraní kontrolní bity a tím získá původní informaci. *Dekodér lineárního kódu*

Pokud $\mathbf{H} \cdot \boldsymbol{w}^T$ není nulový vektor, dekodér má jistotu, že došlo k chybě a že $\boldsymbol{w}$ není kódové slovo. Má-li chybu opravit, pak údaj $\mathbf{H} \cdot \boldsymbol{w}^T$ bude při opravě potřebovat. Napíšeme-li výsledek násobení $\mathbf{H} \cdot \boldsymbol{w}^T$ do řádku, dostáváme tzv. *syndrom* vektoru $\boldsymbol{w}$.

10.49. Definice. Nechť $\mathbf{H}$ je kontrolní matice lineárního kódu. *Syndrom* slova $\boldsymbol{w}$ je vektor $\boldsymbol{s}$, pro který platí $\boldsymbol{s}^T = \mathbf{H} \cdot \boldsymbol{w}^T$.

Nechť $\boldsymbol{v}$ je slovo vyslané kodérem a $\boldsymbol{w}$ je slovo přijaté dekodérem. Pak $\boldsymbol{e} = \boldsymbol{w} - \boldsymbol{v}$ je *chybové slovo*. Protože v $\mathbf{Z}_2^n$ je $-\boldsymbol{v} = \boldsymbol{v}$, chybové slovo lze počítat jako $\boldsymbol{w} + \boldsymbol{v}$.

10.50. Poznámka. Jedničkové bity chybového slova označují místa, kde došlo k poškození slova $\boldsymbol{v}$. Úkolem dekodéru je na základě znalosti $\boldsymbol{w}$ zjistit chybové slovo $\boldsymbol{e}$. Pokud se mu to podaří, pak vypočte původní informaci jako $\boldsymbol{v} = \boldsymbol{w} - \boldsymbol{e}$.

Než se pustíme do sestavování tabulky, podle které bude dekodér opravovat chyby, je potřeba si uvědomit platnost dvou tvrzení. První z nich platí dokonce obecně na libovolném lineárním prostoru.

10.51. Věta. Nechť K je lineární podprostor lineárního prostoru L a nechť $\boldsymbol{e}_1 \in L$, $\boldsymbol{e}_2 \in L$. Pak množiny $M_1 = \{\boldsymbol{e}_1 + \boldsymbol{v};\ \boldsymbol{v} \in K\}$, $M_2 = \{\boldsymbol{e}_2 + \boldsymbol{v};\ \boldsymbol{v} \in K\}$ jsou buď disjunktní nebo totožné.

Důkaz. Sporem. Předpokládáme, že množiny M_1 a M_2 mají společný bod $\boldsymbol{a}$ a přitom nejsou totožné, tj. existuje vektor $\boldsymbol{b} \in M_1$, který neleží v M_2. Protože $\boldsymbol{a}$ i $\boldsymbol{b}$ leží v množině M_1, je $\boldsymbol{a} = \boldsymbol{e}_1 + \boldsymbol{u}$, $\boldsymbol{b} = \boldsymbol{e}_1 + \boldsymbol{v}$, kde $\boldsymbol{u}$ i $\boldsymbol{v}$ leží v K. Pak $\boldsymbol{w} = \boldsymbol{b} - \boldsymbol{a} = \boldsymbol{v} - \boldsymbol{u}$ leží v K, protože K je podprostor. Je tedy $\boldsymbol{b} = \boldsymbol{a} + \boldsymbol{w}$. Protože $\boldsymbol{a}$ leží i v množině M_2, je $\boldsymbol{a} = \boldsymbol{e}_2 + \boldsymbol{x}$, kde $\boldsymbol{x} \in K$. Dosadíme-li tento poznatek do vztahu pro $\boldsymbol{b}$, dostaneme $\boldsymbol{b} = \boldsymbol{e}_2 + \boldsymbol{x} + \boldsymbol{w}$. Protože K je podprostor, $\boldsymbol{x} + \boldsymbol{w}$ leží v K. Je tedy $\boldsymbol{b} = \boldsymbol{e}_2 + \boldsymbol{z}$, kde $\boldsymbol{z} \in K$. To ale znamená, že $\boldsymbol{b} \in M_2$, což je sporu s předpokladem.

10.52. Věta. Nechť $\boldsymbol{v}$ je kódové slovo a $\boldsymbol{e}$ je libovolné slovo. Pak slova $\boldsymbol{e}$ i $\boldsymbol{e} + \boldsymbol{v}$ mají stejný syndrom. Jinými slovy kódová slova modifikovaná stejnou chybou vytvářejí skupinu slov se společným syndromem.

Důkaz. $\mathbf{H} \cdot (\boldsymbol{e} + \boldsymbol{v})^T = \mathbf{H} \cdot \boldsymbol{e}^T + \mathbf{H} \cdot \boldsymbol{v}^T = \mathbf{H} \cdot \boldsymbol{e}^T + \boldsymbol{o}^T = \mathbf{H} \cdot \boldsymbol{e}^T$.

10.53. Poznámka. Pokud požadujeme nejen detekci, ale i opravu chyb lineárního kódu, může dekodér pracovat s následující *tabulkou pro opravování chyb*:

$$\begin{array}{c|ccccc}
\boldsymbol{o} & \boldsymbol{o} & \boldsymbol{v}_2 & \boldsymbol{v}_3 & \dots & \boldsymbol{v}_{2^k} \\
\boldsymbol{s}_2 & \boldsymbol{e}_2 & \boldsymbol{e}_2 + \boldsymbol{v}_2 & \boldsymbol{e}_2 + \boldsymbol{v}_3 & \dots & \boldsymbol{e}_2 + \boldsymbol{v}_{2^k} \\
\boldsymbol{s}_3 & \boldsymbol{e}_3 & \boldsymbol{e}_3 + \boldsymbol{v}_2 & \boldsymbol{e}_3 + \boldsymbol{v}_3 & \dots & \boldsymbol{e}_3 + \boldsymbol{v}_{2^k} \\
\dots & \dots & & & & \\
\boldsymbol{s}_{2^{(n-k)}} & \boldsymbol{e}_{2^{(n-k)}} & \boldsymbol{e}_{2^{(n-k)}} + \boldsymbol{v}_1 & \boldsymbol{e}_{2^{(n-k)}} + \boldsymbol{v}_2 & \dots & \boldsymbol{e}_{2^{(n-k)}} + \boldsymbol{v}_{2^k}
\end{array}$$

Vlevo od svislé čáry jsou syndromy, k těm se vrátím později. Nejprve vysvětlím obsah tabulky vpravo od svislé čáry. Tam jsou rozmístěna všechna slova lineárního prostoru $\mathbf{Z}_2^n$. V prvním řádku jsou kódová slova (je jich 2^k) a v ostatních řádcích jsou slova nekódová. Počet řádků je $2^{(n-k)}$, protože tak získáme celkový počet slov $2^n = 2^k \cdot 2^{(n-k)}$. V prvním sloupci (vpravo od čáry) je nahoře umístěno nulové slovo a pod ním jsou postupně všechna chybová slova, která chceme, aby dekodér uměl odhalit a chybu opravit. Na ostatních pozicích tabulky jsou součty chybového slova v řádku s kódovým slovem ve sloupci.

Tabulku vytvoříme tak, že zapíšeme nejprve do prvního řádku nulové kódové slovo a pak ostatní kódová slova (na pořadí nezáleží). Do druhého řádku napíšeme nejprve chybové slovo, které chceme dekodérem opravovat, a dále příslušné součty. Chybové slovo nesmí být slovem kódovým. Na třetím řádku napíšeme další chybové slovo. Toto chybové slovo se *nesmí vyskytovat nikde na předchozích řádcích.* K němu do řádku doplníme příslušné součty. Tak postupujeme dále, až vytvoříme tabulku s $2^{(n-k)}$ řádky.

První řádek tabulky obsahuje lineární prostor K, druhý řádek tabulky obsahuje množinu $K + \boldsymbol{e}_2$, která je podle věty 10.51 disjunktní s K. Platí totiž $\boldsymbol{e}_2 \notin K$. Třetí řádek obsahuje množinu $K + \boldsymbol{e}_3$, která je disjunktní s K i s $K + \boldsymbol{e}_2$, protože $\boldsymbol{e}_3 \notin K$ a $\boldsymbol{e}_3 \notin K + \boldsymbol{e}_2$, takže můžeme dvakrát použít větu 10.51. A tak dále. Slova v jednom řádku jsou samozřejmě různá. Máme tedy zaručeno, že žádné slovo se v tabulce neopakuje a že jsou vyčerpána všechna slova prostoru $\mathbf{Z}_2^n$.

Pokud nyní dekodér přijme slovo $\boldsymbol{w}$, vyhledá ho v tabulce. Například slovo našel na i-tém řádku tabulky. Dekodér na základě toho rozhodne, že došlo k chybě $\boldsymbol{e}_i$ a opraví ji tak, že provede $\boldsymbol{w} - \boldsymbol{e}_i$. (Místo odčítání může vykonat $\boldsymbol{w} + \boldsymbol{e}_i$, protože v aritmetice $\mathbf{Z}_2$ to dopadne stejně). Pokud $\boldsymbol{w}$ bylo na j-tém sloupci tabulky, dekodér se tímto postupem vrací ke kódovému slovu $\boldsymbol{v}_j$.

Aby dekodér nemusel prohledávat celou tabulku o 2^n slovech, vypočte nejdříve syndrom přijatého vektoru: $\boldsymbol{s}^T = \mathbf{H} \cdot \boldsymbol{w}^T$. Vlevo od svislé čáry jsou syndromy všech slov, které jsou napsány vpravo na stejném řádku (viz věta 10.52). Prohledáním tabulky syndromů a porovnáním se syndromem slova $\boldsymbol{w}$ dekodér odhalí správně řádek tabulky, ve kterém slovo $\boldsymbol{w}$ leží. Dekodér tedy nemusí pracovat s celou tabulkou, ale jen se sloupcem syndromů a sloupcem chybových slov.

10.54. Příklad. Než se pustíme do formulace požadavků na ideální kód pro opravu chyb, zkusíme sestavit tabulku pro opravování chyb pro případ kódů, kde to nebude příliš užitečné: kód s kontrolním bitem parity a opakovací kód. Tím odhalíme problémy, kterých bychom se měli při návrhu kódů s opravou chyb vyvarovat.

Lineární (4,3) kód s kontrolním bitem parity má například tuto tabulku pro opravování chyb:

0	0000	0011	0101	0110	1001	1010	1100	1111
1	1000	1011	1101	1110	0001	0010	0100	0111

V této tabulce jsme zvolili chybové slovo 1000. Proto dekodér při obdržení nekódového slova opraví první bit. Kdybychom zvolili jiné chybové slovo (např. 0100), dostaneme jinou tabulku: druhý řádek bude obsahovat slova v jiném pořadí. Dekodér podle takové pozměněné tabulky bude po přijetí nekódového slova opravovat jiný bit. Bohužel, nemáme žádnou záruku, že dekodér opraví správný bit. Tabulka určuje pevně jeden bit, který bude dekodér opravovat. Lepší by bylo, kdybychom v prvním sloupci s chybovými slovy měli zapsána všechna chybová slova tvaru 1000, 0100, 0010, 0001. To bychom ale potřebovali mít v tabulce pět řádků a ne jen dva. Dva řádky v tabulce jsou důsledkem toho, že kód pracuje jen s jedním kontrolním bitem a že $2^1 = 2$. Můžeme tedy říci, že pro úspěšnou opravu chyb je jeden kontrolní bit málo. To ostatně člověk intuitivně tuší i bez sestavování tabulek pro opravování chyb.

Lineární (6,3) opakovací kód s kontrolní i generující maticí

$$\mathbf{H} = \mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

může mít například následující tabulku pro opravování chyb:

000	000000	100100	010010	001001	110110	011011	101101	111111
100	100000	000100	110010	101001	010110	111011	001101	011111
010	010000	110100	000010	011001	100110	001011	111101	101111
001	001000	101100	011010	000001	111110	010011	100101	110111
110	110000	010100	100010	111001	000110	101011	011101	001111
101	101000	001100	111010	100001	011110	110011	000101	010111
011	011000	111100	001010	010001	101110	000011	110101	100111
111	111000	011100	101010	110001	001110	100011	010101	000111

Pokud dekodér pracuje podle této tabulky a přijme například slovo 111110, vypočte nejdříve syndrom $\mathbf{H} \cdot (111110)^T = (001)^T$, Dekodér zjistil, že slovo leží ve čtvrtém řádku tabulky. Tam je zvoleno chybové slovo 001000, takže dekodér opraví třetí bit a z přijatého slova 111110 dostává kódové slovo 110110.

Jestliže předpokládáme, že přijaté slovo obsahuje jednu chybu, pak výše uvedená oprava nemusí být jediná možná. Opravou posledního bitu ve slově 111110 také dostáváme kódové slovo 111111. Problém tohoto kódu z pohledu tabulky pro opravování chyb je, že chybová slova s jednou jedničkou se objeví dvě na společném řádku tabulky. Na dalších řádcích (za čtvrtým řádkem) už nemůžeme použít chybové slovo 000001, protože toto slovo se na čtvrtém řádku už objevilo. Pokud bychom na čtvrtém řádku použili chybové slovo 000001, pak by se na tomto řádku zase vyskytlo i 001000. Množina slov vedle konkrétního syndromu se totiž nemůže změnit, protože se jedná o množinu řešení soustavy $\mathbf{H}\boldsymbol{x}^T = \boldsymbol{s}^T$. Takže bychom dostali sice jinou tabulku pro opravování chyb, ale chybová slova s jednou jedničkou by se ani tak nepodařilo oddělit do jednotlivých řádků. Ačkoli (na rozdíl od kódu s kontrolním bitem parity) máme v tabulce dostatečný počet řádků, nemáme možnost dostat všechna chybová slova s jednou jedničkou do prvního sloupce tabulky. Dokonce jsme nuceni na posledním řádku tabulky použít chybové slovo se třemi jedničkami.

10.55. Poznámka. Nezdary při opravování chyb v předchozím příkladě nás inspirují k formulaci podmínek na kód, který spolehlivě opravuje jednu chybu.

Předpokládáme lineární (n, k) kód. Chybových slov s jednou jedničkou je n a potřebujeme je všechna rozmístit do prvního sloupce tabulky pro opravování chyb. Žádná jiná chybová slova se v tomto sloupci nesmějí objevit. Z toho vyplývá, že počet řádků tabulky musí být $n + 1$ (první řádek tabulky obsahuje samotný kód). Protože počet řádků tabulky je $2^{(n-k)}$, máme podmínku $2^{(n-k)} = n+1$. Označíme-li počet kontrolních bitů $c = n - k$, pak je uvedená podmínka asi lépe čitelná ve tvaru $n = 2^c - 1$. Celkový počet bitů n tedy musí být o jedničku menší než mocnina dvojky a hodnota této mocniny udává počet kontrolních bitů. Postupně pro $c = 2, 3, 4, 5, 6, \ldots$ dostáváme (3,1), (7,4), (15,11), (31,26), (63,57), ... kódy.

Abychom mohli rozmístit všechna chybová slova s jednou jedničkou do prvního sloupce, potřebujeme ještě zaručit, že žádné slovo s jednou jedničkou není kódové slovo a že dvě slova s jednou jedničkou nebudou mít stejný syndrom. Tuto podmínku nejlépe charakterizuje následující věta.

10.56. Věta. Slovo s jednou jedničkou je kódové právě tehdy, když kontrolní matice obsahuje nulový sloupec. Dvě různá slova s jednou jedničkou mají společný syndrom právě tehdy, když kontrolní matice obsahuje aspoň dva stejné sloupce.

Důkaz. Stačí si uvědomit, že syndrom slova s jednou jedničkou na i-tém místě je roven i-tému sloupci kontrolní matice. To vyplývá z maticového násobení $\mathbf{H} \cdot \boldsymbol{w}^T = \boldsymbol{s}^T$.

10.57. Poznámka. Aby lineární (n, k) kód opravoval všechny jednoduché chyby ve slově, je podle poznámky 10.55 nutné, aby $n = 2^c - 1$, kde $c = n - k$, a dále podle věty 10.56 je nutné, aby kontrolní matice neměla žádný sloupec nulový a všechny sloupce od sebe vzájemně různé. Těch sloupců musí být $n = 2^c - 1$, a přitom výška sloupce je c. Z toho nám vyplývá jediný možný tvar kontrolní matice (až na pořadí sloupců): v jednotlivých sloupcích kontrolní matice napíšeme ve dvojkové soustavě všechna čísla $1, 2, 3, \ldots, n$. Lineárnímu kódu s takovou kontrolní maticí říkáme *Hammingův kód.*

Hammingův kód

10.58. Příklad. Ukážeme si Hammingův $(7, 4)$ kód. Podle předchozí poznámky napíšeme ve dvojkové soustavě do sloupců kontrolní matice čísla 1,2,3,4,5,6,7:

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

Syndromy a první sloupec tabulky pro opravování chyb napíšeme (kvůli úspoře místa v tomto textu) místo do sloupců do řádků:

000	001	010	011	100	101	110	111
0000000	1000000	0100000	0010000	0001000	0000100	0000010	00000001

Vidíme, že při této volbě pořadí sloupců kontrolní matice má dekodér výrazně usnadněnou práci: nemusí prohledávat v tabulce syndromů, aby zjistil odpovídající chybové slovo. Stačí, aby interpretoval syndrom jako číslo zapsané ve dvojkové soustavě. Toto číslo udává pozici bitu chybového slova, kde se nalézá jednička.

Jak tedy bude dekodér postupovat při obdržení slova $\boldsymbol{w}$? Vypočte syndrom pomocí $\boldsymbol{s}^T = \mathbf{H} \cdot \boldsymbol{w}^T$ a interpretuje jej jako číslo i ve dvojkové soustavě. Je-li $i = 0$, je $\boldsymbol{w}$ kódové slovo a dekodér nic neopravuje. Je-li $i > 0$, pak dekodér opraví v obdrženém slově i-tý bit.

Tím je kompletně navržen dekodér Hammingova $(7, 4)$ kódu a zbývá ještě navrhnout kodér. Eliminací kontrolní matice přecházíme ke kontrolní matici stejného kódu (poznámka 10.44):

$$\mathbf{H} = \begin{pmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \end{pmatrix} \sim \begin{pmatrix} 1&0&1&1&0&1&0 \\ 1&1&0&0&1&1&0 \\ 1&0&1&0&1&0&1 \end{pmatrix} \sim \begin{pmatrix} 0&1&1&1&1&0&0 \\ 1&1&0&0&1&1&0 \\ 1&0&1&0&1&0&1 \end{pmatrix} \sim \begin{pmatrix} 0&1&1&1&1&0&0 \\ 1&0&1&1&0&1&0 \\ 1&1&0&1&0&0&1 \end{pmatrix} = \mathbf{H}'.$$

Podle věty 10.43 se tedy jedná o systematický kód, protože $\mathbf{H}' = (\mathbf{C}^T|\mathbf{E}')$. Podle poznámky 10.41 nyní přejdeme ke generující matici $\mathbf{G} = (\mathbf{E}|\mathbf{C})$:

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

Kodér necháme nejprve kopírovat první čtyři informační bity do výstupu a další tři kontrolní bity $\boldsymbol{v}'$ počítáme ze vstupního slova $\boldsymbol{u}$ podle poznámky 10.47:

$$\boldsymbol{v}' = \boldsymbol{u} \cdot \begin{pmatrix} 0&1&1 \\ 1&0&1 \\ 1&1&0 \\ 1&1&1 \end{pmatrix}.$$

10.59. Poznámka. Analogicky se postupuje při návrhu $(15, 11)$, $(31, 26)$, $(63, 57)$ atd. Hammingových kódů. Všimněte si, že s rostoucím n se výrazně zlepšuje poměr informačních bitů ku celkovému počtu přenášených bitů. To je pro uživatele, kteří se zajímají jen o informační bity, dobrá zpráva. Ovšem prodlužováním délky přenášených slov se zase zvyšuje pravděpodobnost výskytu více než jedné chyby ve slově. Dekodér Hammingova kódu v takovém případě selže.

Rozšířený Hammingův kód

10.60. Poznámka. Ve výpočetní technice se pracuje s přenosy 8 bitů, 16 bitů, 32 bitů atd. Hammingův kód předpokládá přenos slov délky o jeden bit kratší. Co se zbylým bitem? Použijeme jej pro kontrolu parity. Tím dostáváme *rozšířený Hammingův kód*, který umožní spolehlivě opravit jednu chybu a detekovat chyby dvě.

10.61. Příklad. K Hammingovu kódu $(7, 4)$ přidáme kontrolní bit parity a dostáváme lineární $(8, 4)$ kód s následující kontrolní maticí:

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

Tento kód umí opravit jednu chybu ve slově a detekovat chyby dvě. Jak dekodér může postupovat? Přijme slovo $\boldsymbol{w}$ a vypočte syndrom $\boldsymbol{s}^T = \mathbf{H} \cdot \boldsymbol{w}^T$. Je-li syndrom nulový vektor, je slovo $\boldsymbol{w}$ kódové a dekodér nic neopravuje. Jsou-li první tři bity syndromu nulové a poslední nenulový, došlo při přenosu jen k chybě posledního kontrolního bitu parity. Je-li na prvních třech pozicích syndromu aspoň jeden bit nenulový a poslední bit syndromu je rovněž nenulový, došlo k lichému počtu chyb ve slově. Dekodér předpokládá, že došlo k jediné chybě a podle prvních třech bitů syndromu zjistí, který bit ve slově má opravit (stejně jako v příkladu 10.58). Je-li konečně poslední bit syndromu nulový, ale syndrom obsahuje aspoň jeden nenulový bit, pak došlo k sudému počtu chyb. Tento počet chyb neumí dekodér opravit, ale detekuje tento stav jako dvojnásobnou chybu.

10.62. Poznámka. Všimněte si, že nejmenší Hammingova vzdálenost mezi dvěma slovy rozšířeného Hammingova kódu je 4. To je v souladu s výsledky příkladu 10.23.

11. Literatura

[1] J. Adámek, *Foundations of Coding.* A Wiley-Interscience publication, New York 1991.

[2] V. Bartík, *Úvod do algebry.* Text k přednášce 1996 na `http://math.feld.cvut.cz/bartik/`.

[3] H.–J. Bartsch, *Matematické vzorce.* Academia, Praha 2006 (4. vydání).

[4] R. A. Beezer, *A First Course in Linear Algebra.* Tacoma, Washington, USA 2007. Text je mj. volně dostupný na `http://linear.ups.edu/`.

[5] L. Bican, *Lineární algebra a geometrie.* Academia, Praha 2002.

[6] G. Birkhoff, S. MacLane, *Algebra.* Chelsea Pub Co, (3rd edition) 1993. Existuje slovenský překlad staršího vydání *Prehľad modernej algebry*, Alfa, Bratislava, 1979.

[7] M. Demlová, B. Pondělíček, *Úvod do algebry.* Vydavatelství ČVUT, Praha 1996.

[8] I. M. Gelfand, *Lineární algebra.* Překlad M. Fiedler, ČSAV, Praha 1953.

[9] J. Hefferon, *Linear Algebra.* Colchester, Vermont USA, volně dostupné na `http://joshua.smcvt.edu/linearalgebra/`.

[10] S. Jílková, V. Maňasová, Z. Tischerová, *Lineární algebra – úlohy.* Vydavatelství ČVUT, Praha 1987.

[11] A. Kalousová, *Skripta z algebry.* Text volně dostupný například z `http://math.feld.cvut.cz/kalous/algebra.html`

[12] T. Kepka, *Algebra.* Poznámky z přednášek na MFF UK dostupné např. na `http://lucy.troja.mff.cuni.cz/labtf/poznamky/`.

[13] V. Kořínek, *Základy algebry.* Klasická učebnice algebry, Academia, Praha 1956 (2. vydání).

[14] E. Krajník, *Základy maticového počtu.* Vydavatelství ČVUT, Praha 2006.

[15] V. Mahel & kol. kat. matematiky, *Sbírka úloh z lineární algebry a analytické geometrie.* Vydavatelství ČVUT, Praha 1986.

[16] J. Matoušek, *Šestnáct miniatur.* Volně dostupný text s aplikacemi lineární algebry tam, kde bychom to možná nečekali, `http://kam.mff.cuni.cz/ matousek/la1.html`.

[17] L. Motl, M. Zahradník, *Pěstujeme lineární algebru.* MFF UK, Praha 1994 (skriptum přístupné na `http://www.kolej.mff.cuni.cz/~lmotm275/skripta/`).

[18] P. Olšák, *Úvod do algebry, zejména lineární.* FEL ČVUT, Praha 2007.

[19] P. Olšák, *TeXbook naruby.* Konvoj, Brno 2001 (2. vydání). Text volně dostupný například na `http://petr.olsak.net/tbn.html`.

[20] L. Procházka, *Algebra.* Academia, Praha 1990.

[21] I. V. Proskurjakov, *Sbornik zadač po linějnoj algebre.* Uzdavatělstvo Nauka, Moskva 1970.

[22] P. Pták, *Introduction to Linear Algebra.* Vydavatelství ČVUT, Praha 2006.

[23] K. Rektorys, *Přehled užité matematiky.* Prometheus, Praha 2003 (6. vydání).

[24] P. Vopěnka, *Úhelný kámen evropské vzdělanosti a moci – rozpravy s geometrií.* Práh, Praha 2003.

[25] K. Výborný, M. Zahradník & kol. *Sbírka příkladů z lineární algebry.* Volně dostupný text k nalezení například na `http://www.kolej.mff.cuni.cz/~lmotm275/skripta/`.

[26] J. Žára, B. Beneš, J. Sochor, P. Felkel, *Moderní počítačová grafika.* Computer Press, 2005 (2. vydání).

[27] Rozcestník volně dostupných textů k algebře v češtině: `http://home.pf.jcu.cz/~novakp08/Matematika/Algebra.htm`.

12. Rejstřík

12.1. Poznámka. Na rozdíl od běžných rejstříků tento neodkazuje na čísla stran, ale na čísla odstavců. To by mělo čtenáři umožnit rychleji najít slovo z rejstříku v textu, protože cíl odkazu je přesnější: text odstavce je typicky menší než text celé strany.

Až na výjimky nejsou v rejstříku pojmy odkazovány na všechna místa, kde se vyskytují. Například pojem „lineární prostor“ nebo „matice“ by asi musel obsahovat odkazy na skoro všechny odstavce. To by ztratilo smysl. Často používané pojmy jsou tedy v rejstříku odkazovány jen na místa, kde jsou definovány nebo kde jsou uvedeny jejich důležité vlastnosti.