

Podpůrné materiály pro studium lineární algebry

David Janíček

Bakalářská práce
2018



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **David Janíček**
Osobní číslo: **A15259**
Studijní program: **B3902 Inženýrská informatika**
Studijní obor: **Informační technologie v administrativě**
Forma studia: **prezenční**

Téma práce: **Podpůrné materiály pro studium lineární algebry**
Téma anglicky: **Study Materials for the Linear Algebra Course**

Zásady pro vypracování:

1. Uvedte základní pojmy z lineární algebry.
2. Vysvětlete základní postupy a vztahy daného tématu.
3. Tyto postupy aplikujte na výpočet ilustrativních příkladů.
4. Demonstrujte využití lineární algebry v dalších oborech za pomoci matematického softwaru.
5. Práci doplňte o dokumentaci k tomuto matematickému softwaru a základní teorii ke zmíněným oborům.

Rozsah bakalářské práce: -

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. BICAN, L. Lineární algebra a geometrie. Academia-nakladatelství Akademie věd ČR, 2002.
2. HORT, D., RACHŮNEK, J. Algebra I. Olomouc: Univerzita Palackého, 2003.
3. EMANOVSKÝ, P., KŮHR, J. Cvičení z algebry pro 1. ročník I. Olomouc: Univerzita Palackého v Olomouci, 2007.
4. MOTL, L., ZAHRADNÍK, M. Pěstujeme lineární algebru. 3. vyd. Praha: Univerzita Karlova v Praze, nakladatelství Karolinum, 2002
5. OLŠÁK, P., Úvod do algebry, zejména lineární. FEL ČVUT, Praha 2007.
6. BEEZER, Robert Arnold. A first course in linear algebra. Beezer, 2008.
7. HEFFERON, J. Linear Algebra 3rd Edition. ISBN-13: 978-1944325039.
8. PTÁK, Pavel. Introduction to linear algebra. 3. vydání. V Praze: České vysoké učení technické, 2017.

Vedoucí bakalářské práce:

Mgr. Jan Krňávek, PhD.

Ústav matematiky

Datum zadání bakalářské práce:

1. prosince 2017

Termín odevzdání bakalářské práce:

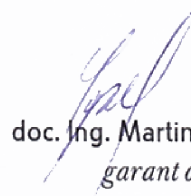
25. května 2018

Ve Zlíně dne 14. prosince 2017



doc. Mgr. Milan Adámek, Ph.D.

děkan



doc. Ing. Martin Sysel, Ph.D.

garant oboru

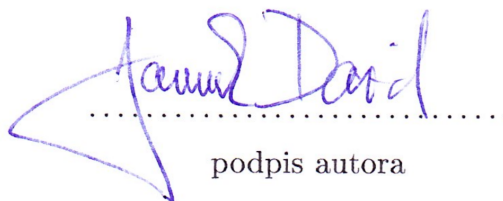
Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářské práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky. Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnaní případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně 22.5.2018


.....
podpis autora

ABSTRAKT

Bakalářská práce je zaměřena na podporu výuky lineární algebry a na následné využití teorie v matematickém software Wolfram Mathematica. Vytvořený text bude součástí materiálů Math Support Centre Univerzity Tomáše Bati a bude součástí také jeho internetových stránek. V práci představuji teorii, týkající se lineární algebry nutnou k pochopení dané problematiky. Dále uvádím přehled matematických nástrojů použitého software, popisuji jejich všeobecné vlastnosti, které demonstruji na ilustrativních příkladech.

V kapitole věnované využití lineární algebry uvádím příklady disciplín, ve kterých se teorie lineární algebry využívá v praxi. Text je doplněn o názorné ukázky vytvořené v programu Wolfram Mathematica.

Klíčová slova: matematika, lineární algebra, Wolfram Mathematica

ABSTRACT

This thesis is focused on support of linear algebra teaching and the subsequent use of theory in the mathematical software Wolfram Mathematica. This text will be a part of materials in Math Support centre at Tomas Bata University and will be a part of its website. In my thesis I present the theory of linear algebra necessary to understand the given problem. As next part I overview math tools, describe their general features and show how to use them on examples.

In chapter about utilization of linear algebra I use examples of disciplines in which is linear algebra theory used in practice. The text is supplemented by visual demonstrations created in Wolfram Mathematica.

Keywords: mathematics, linear algebra, Wolfram Mathematica

Poděkování

Touto cestou bych rád poděkoval panu Mgr. Janu Krňávkovi, Ph.D. za odborné vedení, cenné rady a velkou vstřícnost při vedení mé bakalářské práce.

OBSAH

ÚVOD	9
1 VEKTOROVÉ PROSTORY	10
1.1 ZÁKLADNÍ POJMY A DEFINICE.....	10
1.2 PŘÍKLADY VEKTOROVÝCH PROSTORŮ	13
1.3 LINEÁRNÍ KOMBINACE VEKTORŮ	13
2 MATICE.....	16
2.1 ČÍSELNÉ MATICE	16
2.2 DRUHY MATIC.....	18
2.3 ZÁKLADNÍ OPERACE S MATICEMI.....	19
2.3.1 Sčítání matic.....	19
2.3.2 Násobení matic skalárem	21
2.3.3 Násobení matic	22
2.4 ELEMENTÁRNÍ ÚPRAVY MATIC.....	24
3 DETERMINANTY	28
3.1 PERMUTACE.....	28
3.2 DETERMINANT ČTVERCOVÝCH MATIC.....	30
3.2.1 Vlastnosti determinantu	30
3.3 VÝPOČET DETERMINANTŮ	31
3.3.1 Determinant matice 1. stupně	31
3.3.2 Determinant matice 2. stupně	31
3.3.3 Determinant matice 3. stupně	32
3.3.4 Determinant matice 4. stupně	33
3.4 INVERZNÍ MATICE.....	35
4 SOUSTAVY LINEÁRNÍCH ROVNIC.....	39
4.1 HODNOST MATICE	39
4.2 ŘEŠENÍ SOUSTAV LINEÁRNÍCH ROVNIC	40
5 VYUŽITÍ LINEÁRNÍ ALGEBRY V PRAXI	47
5.1 ŠIFROVÁNÍ.....	47
5.1.1 Hillova šifra v prostředí Wolfram Mathematica	48
5.1.2 Demonstrace Hillovy šifry na příkladu.....	51
5.2 GEOMETRICKÉ TRANSFORMACE	52
5.2.1 Homogenní souřadnice	52
5.2.2 Dvourozměrné geometrické transformace	53

5.2.3	Skládání transformací	55
5.2.4	Grafické transformace v programu Wolfram Mathematica.....	55
ZÁVĚR		66
SEZNAM POUŽITÉ LITERATURY		67
SEZNAM OBRÁZKŮ		69
SEZNAM PŘÍLOH		72

ÚVOD

Tato bakalářská práce se zabývá jednou ze základních disciplín matematiky a představuje teorii nezbytnou k pochopení problematiky lineární algebry. Ta je následně aplikována v matematickém software. Pro potřeby této práce byl zvolen program Wolfram Mathematica, jelikož jeho licence je dostupná pro všechny studenty Fakulty aplikované informatiky Univerzity Tomáše Bati. Tento text by měl pomoci studentům, kteří navštěvují Math Support Centre.

Hlavním zdrojem definic a vět použitých v každé kapitole, byly knihy uvedené v doporučené literatuře rozšířené o literaturu uvedenou v seznamu na konci práce. Text je členěn chronologicky a uvedené poučky lze aplikovat i na problémy, které se vyskytují v kapitolách, které následují. U každé definice popisující danou látku je uveden ilustrační řešený příklad, který s ní úzce souvisí a měl by čtenáři osvětlit cestu, jak a proč se dojde k výsledku. Tyto postupy jsou popsány krok po kroku a tak, aby je mohl pochopit i opravdový laik. Pokud je možností jak se dostat ke stejnému a správnému výsledků více, jsou uvedeny i další tyto postupy.

Toto téma jsem si zvolil z toho důvodu, že pro většinu studentů je nejen lineární algebra ale i matematika, jako taková, problém. Pro studenty je těžký přechod z matematiky, která se vyučuje na středních školách, na matematiku vysokoškolskou. Rozdíly se projevují nejvíce mezi absolventy ze středních odborných škol a absolventy z gymnázií, kteří s matematikou nemají sebemenší problém. Studenti se pak učí látku mechanicky a učí se veškeré postupy nazpaměť. Tempo přednášek jim připadá neúnosné a na případné konzultace se raději nedostaví, aby se v očích ostatních neztrapňovali.

Přesně z tohoto důvodu bylo vytvořeno Math Support Centere v přízemí fakulty aplikované informatiky aby mohli tito studenti přijít a nedostatky dohnat a problematiku pochopit. Svojí prací bych chtěl přispět ke zlepšení kvality výuky v tomto centru a rozšířit obzory navštěvujícím. Za řešenými příklady jsou řešeny i obdobné příklady v software Wolfram Mathematica, které by měli také napomoci k lepší efektivitě řešení a slouží hlavně jako ukázka, že ne všechny problémy, které vyvstávají, je nutné řešit složitě.

V poslední kapitole této práce jsou uvedeny ukázky, jak se teorie lineární algebry aplikuje v praxi s ukázkou na jednoduchých příkladech řešených ve Wolfram Mathematica. Součástí je také dokumentace, sloužící k náhledu pokud by při řešení jakéhokoliv příkladu nastal problém.

Označení: V celém textu bude $\mathcal{T} = (T, +, \cdot)$ libovolné komutativní těleso. \mathbb{R} označuje množinu reálných čísel a \mathcal{R} označuje těleso reálných čísel. $\mathcal{V} = (V, +, \mathcal{T}, \cdot)$ bude libovolný vektorový prostor nad tělesem \mathcal{T} . \mathbb{N} se označuje množina přirozených čísel.

1 VEKTOROVÉ PROSTORY

Vektorové prostory jsou klíčovou matematickou strukturou, se kterou se lze setkat i v jiných oborech než je pouze matematika. Prvky vektorového prostoru se nazývají vektory a prvky z tělesa T se nazývají skaláry. Vektory jsou například všechna reálná čísla společně s operacemi sčítání a násobení, uspořádané dvojice reálných čísel s operacemi sčítání a násobení, anebo to mohou být reálné funkce jedné reálné proměnné s operacemi sčítání a násobení funkcí čísel. Pro označení vektorů se používají písmena se šipkou. Vektorovým prostorem je také množina řešení systému homogenních lineárních rovnic, nebo množina matic typu $m \times n$ s operacemi sčítání matic a násobení matic čísel. Vektory se vyskytují se ve fyzice, kde jsou zobrazeny jako síla, zrychlení a rychlost. V této kapitole budou uvedeny definice a řešené příklady, které by měly vést k pochopení problematiky spojené s vektorovými prostory.

1.1 Základní pojmy a definice

Definice 1.1. Vektorovým prostorem nad tělesem \mathcal{T} rozumíme neprázdnou množinu V (množina vektorů), na které musí být definována binární operace sčítání, tj. musí být definováno zobrazení $+: V \times V \rightarrow V$ a zároveň operace násobení vektorů z \mathcal{T} , tj. $\cdot: \mathcal{T} \times V \rightarrow V$. Přitom pro všechna $\vec{u}, \vec{v}, \vec{w} \in V$ a všechna $a, b \in \mathcal{T}$ musí být splněny následující axiomy:

1. $\vec{u} + \vec{v} = \vec{v} + \vec{u}$,
2. $(\vec{u} + \vec{v}) + \vec{w} = \vec{u} + (\vec{v} + \vec{w})$,
3. existuje nulový prvek $\vec{0} \in V$ takový že, $0 \cdot \vec{u} = \vec{0}$ pro každé $\vec{u} \in V$,
4. $a(\vec{u} + \vec{v}) = a\vec{u} + a\vec{v}$
5. $(a + b)\vec{u} = a\vec{u} + b\vec{u}$
6. $a(b\vec{u}) = (ab)\vec{u}$
7. $1 \cdot \vec{u} = \vec{u}$

Pro úplnost, se někdy místo 3 axiomu uvádí následující 2 axiomy:

- 3'. existuje prvek $\vec{0} \in V$ takový, že $0 + \vec{u} = \vec{u}$ pro každé $\vec{u} \in V$
- 3''. ke každému $\vec{u} \in V$ existuje vektor $(-\vec{u}) \in V$ tak, že $\vec{u} + (-\vec{u}) = \vec{0}$.

Definice 1.2. Buď n přirozené číslo. Na množině T^n všech uspořádaných n -tic prvků z množiny T definujeme binární operaci sčítání prvků předpisem

$$(u_1, u_2, \dots, u_n) + (v_1, v_2, \dots, v_n) = (u_1 + v_1, u_2 + v_2, \dots, u_n + v_n)$$

a operaci násobení prvku z T^n prvkem z tělesa \mathcal{T} předpisem

$$r(u_1, u_2, \dots, u_n) = (ru_1, ru_2, \dots, ru_n)$$

Množina T^n spolu s těmito operacemi se nazývá aritmetický vektorový prostor.

Příklad 1.1. Jsou-li $\vec{u}, \vec{v}, \vec{w} \in T^2$ a skaláry $a, b \in T = (T^2, +, \cdot)$. Dokažte, že čtveřice $\mathcal{T}^2 = (T^2, +, \mathcal{T}, \cdot)$ tvoří aritmetický vektorový prostor nad tělesem \mathcal{T} .

$$\vec{u} = (u_1, u_2), \vec{v} = (v_1, v_2), \vec{w} = (w_1, w_2)$$

Operace sčítání je definována: $(u_1, u_2) + (v_1, v_2) = (u_1 + v_1, u_2 + v_2)$.

Operace násobení je definována: $a \cdot (u_1, u_2) = (a \cdot u_1, a \cdot u_2)$

Ověření platnosti axiomů:

1. $(u_1, u_2) + (v_1, v_2) = (v_1, v_2) + (u_1, u_2)$
 $(u_1 + v_1, u_2 + v_2) = (v_1 + u_1, v_2 + u_2)$
2. $[(u_1, u_2) + (v_1, v_2)] + (w_1, w_2) = (u_1, u_2) + [(v_1, v_2) + (w_1, w_2)]$
 $(u_1 + v_1, u_2 + v_2) + (w_1, w_2) = (u_1, u_2) + (v_1 + w_1, v_2 + w_2)$
 $(u_1 + v_1 + w_1, u_2 + v_2 + w_2) = (u_1 + v_1 + w_1, u_2 + v_2 + w_2)$
3. $0 \cdot (u_1, u_2) = (0 \cdot u_1, 0 \cdot u_2) = (0, 0)$
4. $a \cdot [(u_1, u_2) + (v_1, v_2)] = a \cdot (u_1, u_2) + a \cdot (v_1, v_2)$
 $(a \cdot [u_1 + v_1], a \cdot [u_2 + v_2]) = (au_1, au_2) + (av_1, av_2)$
 $(au_1 + av_1, au_2 + av_2) = (au_1 + av_1, au_2 + av_2)$
5. $(a + b) \cdot (u_1, u_2) = a \cdot (u_1, u_2) + b \cdot (u_1, u_2)$
 $([a + b] \cdot u_1, [a + b] \cdot u_2) = (au_1, au_2) + (bu_1, bu_2)$
 $([au_1 + bu_1], [au_2 + bu_2]) = ([au_1 + bu_1], [au_2 + bu_2])$
6. $a \cdot [b \cdot (u_1, u_2)] = (a \cdot b) \cdot (u_1, u_2)$
 $a \cdot (b \cdot u_1, b \cdot u_2) = ([a \cdot b] \cdot u_1, [a \cdot b] \cdot u_2)$
 $(a \cdot [b \cdot u_1], a \cdot [b \cdot u_2]) = ([a \cdot b] \cdot u_1, [a \cdot b] \cdot u_2)$
 $(a \cdot b \cdot u_1, a \cdot b \cdot u_2) = (a \cdot b \cdot u_1, a \cdot b \cdot u_2)$
7. $1 \cdot (u_1, u_2) = (1 \cdot u_1, 1 \cdot u_2) = (u_1, u_2)$

Příklad 1.2. Zjistěte v programu Wolfram Mathematica, zda čtveřice $\mathcal{R}^5 = (\mathbb{R}^5, +, \mathcal{R}, \cdot)$ tvoří vektorový prostor nad tělesem \mathcal{R} jsou-li vektory $\vec{u}, \vec{v}, \vec{w} \in \mathbb{R}^5$ a skaláry $a, b \in \mathbb{R}$.

```

1 In[1] := u = Array[u, 5]
2 In[2] := v = Array[v, 5]
3 In[3] := w = Array[w, 5]
4 In[3] := o = {0, 0, 0, 0, 0}
5
6 Out[1] = {u[1], u[2], u[3], u[4], u[5]}
7 Out[2] = {v[1], v[2], v[3], v[4], v[5]}
8 Out[3] = {w[1], w[2], w[3], w[4], w[5]}
9 Out[3] = {0, 0, 0, 0, 0}

```

Zdrojový kód 1 Definice vektorů $\vec{u}, \vec{v}, \vec{w}$ a skalárů a, b

```

1 In[6] := (u+v) == (v+u)
2 Out[6] = True
3 In[7] := (u+v)+w == u+(v+w)
4 Out[7] = True
5 In[8] := 0*u == o
6 Out[8] = True
7 In[9] := Simplify[a*(u+v) == a*u+a*v]
8 Out[9] = True
9 In[10] := Simplify[(a+b)*u == a*u+b*u]
10 Out[10] = True
11 In[11] := a*(b*u) == (a*b)*u
12 Out[11] = True
13 In[12] := 1*u == u
14 Out[12] = True

```

Zdrojový kód 2 Ověření platnosti axiomů

Z výstupu programu je patrné, že všechny axiomy jsou splněny. Totiž při ověřování podmínek axiomu pomocí funkce **Equal**(==) se vždy vrátila hodnota True.

Čtveřice $\mathcal{R}^5 = (\mathbb{R}^5, +, \mathcal{R}, \cdot)$ tedy tvoří vektorový prostor nad tělesem \mathcal{R} .

1.2 Příklady vektorových prostorů

1. Těleso \mathcal{T} spolu s operacemi sčítání a násobení definovanými na T je zřejmě vektorový prostor nad \mathcal{T} .
2. Speciálně těleso reálných čísel \mathcal{R} je vektorový prostor nad \mathcal{R} . Vektorový prostor nad tělesem \mathcal{R} se nazývá *reálný vektorový prostor*.
3. Těleso komplexních čísel \mathcal{C} je vzhledem k obvyklým operacím sčítání a násobení jak reálný, tak komplexní vektorový prostor.
4. Množina P všech kladných reálných čísel spolu s operacemi \oplus a \odot , kde $u \oplus v = uv$, $r \odot u = u^r$, $u, v \in P$, $r \in \mathbb{R}$, je reálný vektorový prostor.
5. Buď S neprázdná množina a označme T^S množinu všech zobrazení z S do $\mathcal{T} = (T, +, \cdot)$. Definujeme-li pro $f, g \in T^S$, $r \in T$ operace $(f + g)(x) = f(x) + g(x)$ a $(rf)(x) = rf(x)$ pro každé $x \in S$, je množina T^S spolu s těmito operacemi vektorovým prostorem nad \mathcal{T} .

1.3 Lineární kombinace vektorů

Definice 1.3. Vektory $\vec{u}_1, \dots, \vec{u}_k, \vec{v}$ jsou z vektorového prostoru \mathcal{V} , potom řekneme, že \vec{v} je lineární kombinací vektorů $\vec{u}_1, \dots, \vec{u}_k$, existují-li prvky $c_1, \dots, c_k \in T$ taková, že

$$\vec{v} = c_1 \vec{u}_1 + \dots + c_k \vec{u}_k = \sum_{i=1}^k c_i \vec{u}_i.$$

Příklad 1.3. Zjistěte, je-li vektor \vec{v} lineární kombinací vektorů $\vec{u}_1, \vec{u}_2, \vec{u}_3$ pokud platí $\vec{v}, \vec{u}_1, \vec{u}_2, \vec{u}_3 \in \mathbb{R}^3$:

$$\vec{v} = (4, -2, 3), \vec{u}_1 = (2, 1, -2), \vec{u}_2 = (-3, 4, 2), \vec{u}_3 = (1, 0, -3).$$

Musíme zjistit, zda existují reálná čísla c_1, c_2, c_3 taková aby platilo

$$\vec{v} = c_1 \vec{u}_1 + \dots + c_k \vec{u}_k = \sum_{i=1}^k c_i \vec{u}_i.$$

Zjistíme tedy má-li řešení soustava rovnic

$$\begin{aligned} 2c_1 - 3c_2 + c_3 &= 4 \\ c_1 + 4c_2 &= -2 \\ -2c_1 + 2c_2 - 3c_3 &= 3 \end{aligned}$$

V prvním kroku použijeme substituční metodu, tj. z druhé rovnice vyjádříme $c_1 = -4c_2 - 2$ a dosadíme do první a poslední rovnice.

$$-11c_2 + c_3 = 8$$

$$10c_2 - 3c_3 = 3$$

První rovnici vynásobíme 3 a sečteme s rovnicí druhou. Poté dostaneme výslednou hodnotu pro $c_2 = -1$. Tuto hodnotu dosadíme do druhé rovnice ze zadání a dostáváme výslednou hodnotu pro $c_1 = 2$. Zbývá nám už jenom výpočet hodnoty pro c_3 a to z první rovnice $c_3 = -3$.

Výpočtem jsme dostali rovnost $\vec{v} = 2\vec{u}_1 - \vec{u}_2 - 3\vec{u}_3$ a proto můžeme říci, že vektor \vec{v} je lineární kombinací vektorů $\vec{u}_1, \vec{u}_2, \vec{u}_3$.

Příklad 1.4. Zjistěte v programu Wolfram Mathematica, je-li vektor \vec{v} lineární kombinací vektorů $\vec{u}_1, \vec{u}_2, \vec{u}_3$ pokud platí $\vec{v}, \vec{u}_1, \vec{u}_2, \vec{u}_3 \in \mathbb{R}^3$:

$$\vec{v} = (2, -1, 3), \vec{u}_1 = (-5, 2, 1), \vec{u}_2 = (1, -3, 2), \vec{u}_3 = (-3, -4, 5).$$

```

1 In[20]:= u1 = {-5, 2, 1};
2           u2 = {1, -3, 2};
3           u3 = {-3, -4, 5};
4           v = {2, -1, 3};
5 In[20]:= Solve[{c1*u1+c2*u2+c3*u3 == v}, {c1, c2, c3}]
6
7 Out[24]= {}

```

Zdrojový kód 3 Výpočet lineární kombinace vektorů

Tato soustava rovnice tedy nemá řešení. Vektor \vec{v} není lineární kombinací vektorů $\vec{u}_1, \vec{u}_2, \vec{u}_3$.

Definice 1.4. Lineární kombinaci $\sum_{i=1}^k 0\vec{u}_i$ vektorů $\vec{u}_1, \dots, \vec{u}_k$ nazveme triviální nulovou kombinací vektorů $\vec{u}_1 + \dots + \vec{u}_k$.

Definice 1.5. Lineární kombinaci $\sum_{i=1}^k c_i \vec{u}_i$ vektorů $\vec{u}_1, \dots, \vec{u}_k$ v níž je alespoň jeden koeficient c_1, \dots, c_k nenulový, nazveme netriviální kombinací vektorů $\vec{u}_1, \dots, \vec{u}_k$.

Definice 1.6. Řekneme, že vektory $\vec{u}_1, \dots, \vec{u}_k$ z vektorového prostoru \mathcal{V} pro $k \in \mathbb{N}$ jsou lineárně závislé, pokud existuje alespoň jedna jejich netriviální nulová kombinace. V opačném případě jsou vektory lineárně nezávislé.

Příklad 1.5. Zjistěte, zda jsou lineárně závislé nebo nezávislé vektory:

$$\vec{u}_1 = (-2, 4, 1), \vec{u}_2 = (5, 0, -3)$$

Prvním krokem bude přepsání vektorů do soustavy lineárních rovnic.

$$-2c_1 + 5c_2 = 0$$

$$4c_1 = 0$$

$$c_1 - 3c_2 = 0$$

Sčítací metodou lze snadno zjistit, že nelze najít řešení soustavy rovnic, kde by c_1 nebo c_2 bylo různé od nuly.

Tedy vektory \vec{u}_1 a \vec{u}_2 jsou lineárně nezávislé.

Příklad 1.6. Zjistěte v programu Wolfram Mathematica, zda jsou lineárně závislé, nebo nezávislé vektory

$$\vec{u}_1 = (2, -3), \vec{u}_2 = (1, 4), \vec{u}_3 = (4, -17)$$

```
1 In[14]:= u1={2,-3};  
2           u2={1,4};  
3           u3={4,-17};  
4  
5 In[15]:= Solve[{c1*u1+c2*u2+c3*u3==0},{c1,c2,c3}]  
6 Out[15]= {{c2->-(2 c1)/3},c3->-(c1/3)}
```

Zdrojový kód 4 Ověření lineární závislosti

Program nenašel pouze jediné řešení této soustavy rovnic, a výsledek lze interpretovat tak, že pokud si zvolíme hodnotu c_1 libovolně a zároveň bude $c_2 = -\frac{2c_1}{3}$, $c_3 = -\frac{c_1}{3}$ dostaneme z této soustavy vždy řešení odpovídající zadání.

Např. $c_1 = -3$, $c_2 = 2$, $c_3 = 1$.

Vektory $\vec{u}_1, \vec{u}_2, \vec{u}_3$ jsou tedy lineárně závislé.

2 MATICE

Matice patří mezi další základní pojmy lineární algebry a jsou významným prostředkem pro vyjadřování úvah týkající se této problematiky. Za zakladatele teorie matic se považuje anglický matematik A. Cayley (1821–1895) na základě jeho díla [12]. Na dalším rozvoji teorie matic se podíleli zejména G. Frobenius (1849–1917), J. J. Sylvester (1814–1897) a K. Weierstrass (1815–1897). Jednoduše lze říci, že matice je čtvercové, nebo obdélníkové schéma čísel. Tyto čísla se nazývají prvky matice. Obecně tedy obsahuje m řádků a n sloupců, což se matematicky zapisuje jako $m \times n$.

Matice se nejčastěji využívají k vyjádření transformací vektorů, nebo například k výpočtu soustavy lineárních rovnic.

2.1 Číselné matice

Definice 2.1. Nechť $\mathcal{T} = (T, +, \cdot)$ je komutativní těleso a m, n přirozená čísla. Matici typu $m \times n$ nad číselným tělesem \mathcal{T} (zapisuje se jako $A \in M_{m \times n}(\mathcal{T})$) rozumíme zobrazení kartézského součinu $\{1, 2, \dots, m\} \times \{1, 2, \dots, n\}$ do T . Matici zapisujeme nejčastěji ve tvaru tabulky:

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

Nebo i stručněji, pokud je z kontextu jasný počet řádků a počet sloupců matice A , ve tvaru: $A = (a_{ij})$.

Matici typu $m \times n$ tedy lze chápat jako prvky a_{ij} z tělesa \mathcal{T} takové, že i probíhá množinu $\{1, 2, \dots, m\}$ a j probíhá množinu $\{1, 2, \dots, n\}$. Prvky množiny $\{1, 2, \dots, m\}$, tj. levé indexy, se nazývají indexy řádkové a prvky množiny $\{1, 2, \dots, n\}$, tj. pravé indexy se nazývají indexy sloupcové. Pro pevné i budeme i -tým řádkem matice A nazývat n -tice $(a_{i1}, a_{i2}, \dots, a_{in})$. Podobně pro pevné j budeme m -tice $(a_{1j}, a_{2j}, \dots, a_{mj})$ nazývat j -tým sloupcem matice A .

Samotná čísla $a_{ij} \in T$, $1 \leq i \leq m$, $1 \leq j \leq n$, nazýváme prvky matice A .

Příklad 2.1. Je-li matice $A = \begin{pmatrix} 1 & 2 & 4 \\ -3 & 5 & 3 \end{pmatrix}$, pak se jedná o matici se dvěma řádky a třemi sloupci. Prvky nacházející se například v prvním sloupci jsou $a_{11} = 1$ a $a_{21} = -3$.

Označení: Množinu všech matic typu $m \times n$ nad \mathcal{T} označíme $M_{m \times n}(\mathcal{T})$ a množinu všech čtvercových matic stupně n nad \mathcal{T} budeme značit $M_n(\mathcal{T})$.

Příklad 2.2. Vytvořte v programu Wolfram Mathematica matici $A \in M_4(\mathcal{T})$, jejíž prvky budou náhodně vygenerovaná celá čísla a vypište:

- a) prvek a_{12} a prvek a_{22} ,
- b) druhý a třetí řádek matice A,
- c) první a třetí sloupec matice A.

```
1 In[1] := A=RandomInteger[{0,10},{4,4}];  
2 Out[35] := MatrixForm[A]  
3  
4  
5 Out[34] = 
$$\begin{pmatrix} 5 & 9 & 0 & 7 \\ 4 & 5 & 8 & 4 \\ 7 & 3 & 3 & 1 \\ 5 & 2 & 4 & 9 \end{pmatrix}$$
  
6  
7
```

Zdrojový kód 5 Vytvoření matice A

```
1 In[3] := A[[1,2]]  
2 Out[3] = 9  
3 In[4] := Part[A,2,2]  
4 Out[4] = 5
```

Zdrojový kód 6 Vypsání prvku a_{12} a prvku a_{22}

```
1 In[5] := A[[2]]  
2 Out[5] = {4,5,8,4}  
3 In[6] := A[[3]]  
4 Out[6] = {7,3,3,1}
```

Zdrojový kód 7 Vypis druhého a třetího řádku

```
1 In[7] := Part[A,All,1]  
2 Out[20] = {5,4,7,5}  
3 In[8] := Part[A,All,3]  
4 Out[21] = {0,8,3,4}
```

Zdrojový kód 8 Vypis prvního a třetího sloupce

2.2 Druhy matic

Definice 2.2. (Nulová matice) Matice $N \in M_{m \times n}(\mathcal{T})$ se nazývá nulová, platí-li $a_{ij} = 0$ pro každé $i = 1, 2, \dots, m, j = 1, 2, \dots, n$.

Příklad nulové matice:

$$N = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Definice 2.3. (Transponovaná matice) Je-li $A = (a_{ij}) \in M_{m \times n}(\mathcal{T})$, potom maticí transponovanou k matici A nazýváme matici $A^T = (a_{ji}) \in M_{n \times m}(\mathcal{T})$, která vznikne z matice A vzájemnou záměnou řádků a sloupců, tj. překlopením matice A podle hlavní diagonály.

Příklad transponované matice:

$$A = \begin{pmatrix} 0 & 1 & 4 \\ 8 & 5 & 2 \\ 10 & 15 & 6 \end{pmatrix}, \quad A^T = \begin{pmatrix} 0 & 8 & 10 \\ 1 & 5 & 15 \\ 4 & 2 & 6 \end{pmatrix}$$

Definice 2.4. (Čtvercová matice) Čtvercová matice je speciálním typem matic a to z toho důvodu, že počet sloupců je roven počtu řádků, tj. platí $m = n$. Zapisuje se jako $A \in M_n(\mathcal{T})$ a nazývá se čtvercová matice stupně n .

Příklad čtvercové matice:

$$A = \begin{pmatrix} 1 & 4 & 5 \\ 3 & 54 & 2 \\ 6 & 9 & 8 \end{pmatrix}$$

Definice 2.5. (Diagonální matice) Matice $A \in M_n(\mathcal{T})$ se nazývá diagonální, pokud všechny její prvky, které neleží na hlavní diagonále, jsou rovny 0. Hlavní diagonálou rozumíme n -tici $(a_{11}, a_{22}, \dots, a_{nn})$.

Příklad digonální matice:

$$A = \begin{pmatrix} 5 & 0 & 0 \\ 0 & 7 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

Definice 2.6. (Jednotková matice) Matice $E \in M_n(\mathcal{T})$ jejíž prvky na hlavní diagonále jsou rovny 1 a všechny ostatní prvky ležící mimo hlavní diagonálu rovny 0, se nazývá jednotková matice stupně n . Matice, která je násobkem matice jednotkové, je skalární.

Příklad jednotkové a skalární matice:

$$E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} 5 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$

Definice 2.7. (Symetrická matice) Symetrická matice je speciální čtvercovou maticí, která splňuje rovnost $A = A^T$. Tedy prvky symetrické podle hlavní diagonály se rovnají, tj. platí $a_{ij} = a_{ji}$ pro každé $i = 1, \dots, n$, $j = 1, \dots, n$.

Příklad symetrické matice:

$$A = \begin{pmatrix} 9 & 7 & 1 \\ 7 & 5 & 0 \\ 1 & 0 & 2 \end{pmatrix}$$

Definice 2.8. (Antisymetrická matice) Antisymetrická matice je čtvercová matice, která splňuje podobné podmínky jako matice symetrická s tím rozdílem, že prvky symetrické podle hlavní diagonály jsou k sobě vzájemně opačné, tj. platí $a_{ij} = -a_{ji}$ pro každé $i = 1, \dots, n$, $j = 1, \dots, n$.

Příklad antisymetrické matice:

$$A = \begin{pmatrix} 0 & -7 & -1 \\ 7 & 0 & 4 \\ 1 & -4 & 0 \end{pmatrix}$$

2.3 Základní operace s maticemi

2.3.1 Sčítání matic

Definice 2.9. Necht' $A = (a_{ij}) \in M_{m \times n}(\mathcal{T})$, $B = (b_{ij}) \in M_{m \times n}(\mathcal{T})$. Potom součtem matic A a B rozumíme matici $A + B = C = (c_{ij})$ takovou, že $c_{ij} = a_{ij} + b_{ij}$ pro každé $i = 1, \dots, m$, $j = 1, \dots, n$.

Příklad 2.3. Necht'

$$A = \begin{pmatrix} 2 & 5 \\ 1 & 0 \\ 4 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} -3 & 1 \\ 4 & -6 \\ 2 & 8 \end{pmatrix}$$

Součtem matic $A + B$ je tedy

$$A + B = \begin{pmatrix} -1 & 6 \\ 5 & -6 \\ 6 & 11 \end{pmatrix}$$

Operace sčítání matic splňuje podmínky komutativity i asociativity tj. pro libovolné matice $A, B, C \in M_{m \times n}$ platí

1. $A + B = B + A$,
2. $(A + B) + C = A + (B + C)$

Pro nulovou matici N typu $m \times n$ a pro libovolnou matici $A \in M_{m \times n}(\mathcal{T})$ platí:

$$A + N = A = N + A$$

tedy matice N je nulový prvek.

Definice 2.10. Jestliže jsou $A \in M_{m \times n}(\mathcal{T})$, $B \in M_{m \times n}(\mathcal{T})$ a platí vztah $A + B = N$, pak je matice B opačnou maticí k matici A , označená jako $B = (-A)$

Příklad 2.4. Sečtěte v programu Wolfram Mathematica dané matice A, B .

$$A = \begin{pmatrix} 19 & 8 & 13 \\ 5 & -2 & 27 \\ -4 & 15 & 0 \\ 1 & 4 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 9 & -5 \\ 0 & 2 & 11 \\ 1 & -3 & 3 \\ 6 & 14 & 8 \end{pmatrix}$$

```

1 In[1]:=A={{19,8,13},{5,-2,27},{-4,15,0},{1,4,2}};
2       B={{1,9,-5},{0,2,11},{1,-3,3},{6,14,8}};
3 In[2]:= MatrixForm[A+B]
4
5      Out[34]=  $\begin{pmatrix} 20 & 17 & 8 \\ 5 & 0 & 38 \\ -3 & 12 & 3 \\ 7 & 18 & 10 \end{pmatrix}$ 
6
7
8
```

Zdrojový kód 9 Součet dvou matic

Definice 2.11. Nechť $A \in M_{m \times n}(\mathcal{T})$, $B \in M_{m \times n}(\mathcal{T})$. Potom rozdílem matic A a B rozumíme součet matic $A + (-B)$, kde matice $(-B)$ je opačnou maticí k matici B

Příklad 2.5. Nechť

$$A = \begin{pmatrix} 8 & 6 \\ 4 & -2 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 5 & 3 \\ 4 & 2 \\ -3 & 1 \end{pmatrix}$$

Rozdílem matic $A + (-B)$ je tedy

$$A + (-B) = \begin{pmatrix} 3 & 3 \\ 0 & 0 \\ 4 & -1 \end{pmatrix}$$

Příklad 2.6. Odečtěte v programu Wolfram Mathematica dané matice A, B .

$$A = \begin{pmatrix} 19 & 8 & 13 \\ 5 & -2 & 27 \\ -4 & 15 & 0 \\ 1 & 4 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 9 & -5 \\ 0 & 2 & 11 \\ 1 & -3 & 3 \\ 6 & 14 & 8 \end{pmatrix}$$

```

1 In[1]:=A={{19,8,13},{5,-2,27},{-4,15,0},{1,4,2}};
2      B={{1,9,-5},{0,2,11},{1,-3,3},{6,14,8}};
3 In[2]:= MatrixForm[A+(-B)]
4
5      Out[34]=
6      \begin{pmatrix} 18 & -1 & 18 \\ 5 & -4 & 16 \\ -5 & 18 & -3 \\ -5 & -10 & -6 \end{pmatrix}
7
8
```

Zdrojový kód 10 Rozdíl dvou matic

2.3.2 Násobení matic skalárem

Definice 2.12. Nechť je c libovolným prvkem z tělesa \mathcal{T} a matice $A = (a_{ij}) \in M_{m \times n}(\mathcal{T})$. Potom vynásobením matice A skalárem c rozumíme matici $cA = (ca_{ij})$.

Obdobně je možné definovat $Ac = (a_{ij}c)$. Platí $cA = Ac$, protože $ca_{ij} = a_{ij}c$.

Obecně pro libovolné skaláry $c, d \in \mathcal{T}$ a libovolné matice $A, B \in M_{m \times n}(\mathcal{T})$ platí

1. $c(A + B) = cA + cB$,

$$2. (c + d)A = cA + dA,$$

$$3. (cd)A = c(dA),$$

$$4. 1 \cdot A = A$$

Příklad 2.7. Je-li

$$c = 2, \quad A = \begin{pmatrix} -2 & 5 \\ 1 & -1 \\ 0 & 7 \end{pmatrix}$$

pak vynásobením matice A skalárem c rozumíme

$$cA = 2 \cdot \begin{pmatrix} -2 & 5 \\ 1 & -1 \\ 0 & 7 \end{pmatrix} = \begin{pmatrix} -4 & 10 \\ 2 & -2 \\ 0 & 14 \end{pmatrix}$$

Příklad 2.8. Vynásobte v programu Wolfram Mathematica matici A skalárem c , je-li

$$c = 3, \quad A = \begin{pmatrix} 2 & 64 & -6 & 4 \\ 8 & 0 & -18 & 6 \\ 56 & -26 & 14 & 1 \\ 12 & 4 & 0 & 2 \end{pmatrix}$$

```

1 In[1] := c=3;
2      A={ {2, 64, -6, 4}, {8, 0, -18, 6}, {56, -26, 14, 1}, {12, 4, 0, 2} };
3 In[2] := MatrixForm[c*A]
4
5      Out[34] = 
$$\begin{pmatrix} 6 & 192 & -18 & 12 \\ 24 & 0 & -54 & 18 \\ 168 & -78 & 42 & 3 \\ 36 & 12 & 0 & 6 \end{pmatrix}$$

6
7
8
```

Zdrojový kód 11 Násobení matice skalárem

2.3.3 Násobení matic

Definice 2.13. Necht $A = (a_{ij}) \in M_{m \times n}(\mathcal{T})$, $B = (b_{jk}) \in M_{n \times p}(\mathcal{T})$. Potom součinem matic A a B rozumíme matici $A \cdot B = AB = (c_{ik}) \in M_{m \times p}(\mathcal{T})$ takovou, že

$$c_{ik} = \sum_{j=1}^n a_{ij} \cdot b_{jk},$$

pro každé $i = 1, \dots, m$, $k = 1, \dots, p$.

Jednodušeji lze výše uvedený vzorec popsat tak, že prvek c_{ik} (prvek na průsečíku i -tého řádku a k -tého sloupce) se vypočte jako součet součinů každého prvku v i -tém řádku matice A s prvkem v k -tém sloupci matice B . Tento součet tvoří j sčítanců:

$$c_{ik} = \begin{pmatrix} a_{i1} & a_{i2} & \dots & a_{ij} \end{pmatrix} \cdot \begin{pmatrix} b_{1k} \\ b_{2k} \\ \vdots \\ b_{jk} \end{pmatrix} = a_{i1}b_{1k} + a_{i2}b_{2k} + \dots + a_{ij}b_{jk}.$$

Z definice je viditelné, že násobit můžeme pouze matice A, B , je-li počet sloupců matice A stejný jako počet řádků matice B . Je také důležité dávat pozor na pořadí matic, jelikož operace násobení matic není komutativní. Součin AB a BA se tedy obecně nerovnají. Součin BA existuje právě a pouze tehdy, když $m = p$.

Příklad 2.9. Jsou-li

$$A = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 2 & 4 \\ -2 & 3 & 1 & 3 \end{pmatrix}$$

pak součinem AB rozumíme

$$AB = \begin{pmatrix} -5 & 9 & 5 & 13 \\ 0 & 3 & 5 & 11 \end{pmatrix}$$

ale přitom součin BA neexistuje.

Násobení matic je asociativní, tj. pro všechny $A \in M_{m \times n}(\mathcal{T})$, $B \in M_{n \times p}(\mathcal{T})$, $C \in M_{p \times r}(\mathcal{T})$ platí

$$(AB)C = A(BC).$$

Příklad 2.10. Vytvořte v programu Wolfram Mathematica matice $A, B, C \in M_4(\mathcal{T})$ jejichž prvky budou náhodně vygenerována celá čísla. Proveďte součin těchto matic a zároveň ověřte, že pro tyto tři matice platí $(AB)C = A(BC)$.

```

1 In[27] := a=RandomInteger[{0,10},{4,4}]
2           b=RandomInteger[{0,10},{4,4}]
3           c=RandomInteger[{0,10},{4,4}]
4
5 Out[32]={ {2,8,2,9},{10,2,0,5},{8,4,9,1},{4,1,5,1}}
6 Out[32]={ {9,6,10,2},{9,5,1,5},{0,5,3,8},{1,0,8,0}}
7 Out[32]={ {10,5,4,2},{7,4,1,4},{1,2,4,6},{5,1,9,3}}
8
9 In[30] := MatrixForm[(a.b).c]
10
11           
$$\text{Out}[34] = \begin{pmatrix} 1830 & 1015 & 1422 & 1262 \\ 1912 & 1159 & 1360 & 1448 \\ 2540 & 1343 & 1997 & 1708 \\ 1167 & 627 & 971 & 851 \end{pmatrix}$$

12
13
14
15 In[30] := (a.b).c == a.(b.c)
16 Out[30] = True

```

Zdrojový kód 12 Násobení matic

2.4 Elementární úpravy matic

Jestli je matice $A = (a_{ij})$ nad \mathcal{T} typu $m \times n$, pak se řádky matice A můžeme považovat za vektory aritmetického vektorového prostoru T^n .

Definice 2.14. Řádkově elementárními úpravami matice A nazýváme:

1. výměna dvou libovolných řádků v A ,
2. vynásobení i -tého řádku v A číslem $c \in \mathcal{T}$, které je různé od nuly,
3. přičtení libovolného násobku některého řádku z A k jinému řádku v A .

Definice 2.15. Sloupcově elementárními úpravami matice A nazýváme:

1. výměna dvou libovolných sloupců v A
2. vynásobení j -tého sloupce v A číslem $c \in \mathcal{T}$, které je různé od nuly

3. přičtení libovolného násobku některého sloupce z A k jinému sloupci v A

Příklad 2.11. Aplikujte postupně řádkové elementární úpravy na matici A pokud

$$A = \begin{pmatrix} 1 & 5 & 4 \\ 8 & 2 & 7 \\ 9 & 6 & 3 \end{pmatrix}$$

První úpravou je přičtení druhého řádku matice k řádku prvnímu:

$$A = \begin{pmatrix} 9 & 7 & 11 \\ 8 & 2 & 7 \\ 9 & 6 & 3 \end{pmatrix}$$

Druhou úpravou je vynásobení třetího řádku matice číslem 2:

$$A = \begin{pmatrix} 9 & 7 & 11 \\ 8 & 2 & 7 \\ 18 & 18 & 6 \end{pmatrix}$$

Třetí úpravou je přičtení dvojnásobku druhého řádku matice k řádku prvnímu:

$$A = \begin{pmatrix} 25 & 11 & 25 \\ 8 & 2 & 7 \\ 18 & 18 & 6 \end{pmatrix}$$

Příklad 2.12. Aplikujte postupně sloupcové elementární úpravy na matici A v programu Wolfram Mathematica

$$A = \begin{pmatrix} 12 & 9 & 2 \\ 4 & 14 & 7 \\ 8 & 7 & 0 \\ 1 & 19 & -6 \end{pmatrix}$$

1. Přičtete druhý sloupec matice k sloupci třetímu
2. Vynásobte první sloupec matice číslem 2
3. Vyměňte druhý a první sloupec matice

```

1 In[31] := A = {{12, 9, 2}, {4, 14, 7}, {8, 7, 0}, {1, 19, -6}};
2 In[32] := MatrixForm[A[[All, 3]] = A[[All, 2]] + A[[All, 3]]]
3
4      
$$\begin{pmatrix} 11 \\ 21 \\ 7 \\ 13 \end{pmatrix}$$

5 Out[32] =
6
7
8 In[33] := MatrixForm[A]
9
10      
$$\begin{pmatrix} 12 & 9 & 11 \\ 4 & 14 & 21 \\ 8 & 7 & 7 \\ 1 & 19 & 13 \end{pmatrix}$$

11 Out[33] // MatrixForm =
12
13

```

Zdrojový kód 13 Přičtení druhého sloupce matice k sloupci třetímu

```

1 In[34] := A[[All, 1]] = 2 * A[[All, 1]]
2
3 In[35] := MatrixForm[A]
4
5      
$$\begin{pmatrix} 24 & 9 & 11 \\ 8 & 14 & 21 \\ 16 & 7 & 7 \\ 2 & 19 & 13 \end{pmatrix}$$

6 Out[34] =
7
8

```

Zdrojový kód 14 Vynásobení prvního sloupce matice číslem 2

```

1 In[36] := A[[All, {1, 2}]] = A[[All, {2, 1}]]];
2
3 In[37] := MatrixForm[A]
4
5      
$$\begin{pmatrix} 9 & 24 & 11 \\ 14 & 8 & 21 \\ 7 & 16 & 7 \\ 19 & 2 & 13 \end{pmatrix}$$

6 Out[34] =
7
8

```

Zdrojový kód 15 Výměna sloupců matice

Definice 2.16. Jsou-li $A, B \in M_{m \times n}(\mathcal{T})$, pak řekneme, že matice B je řádkově, respektive sloupcově, ekvivalentní s maticí A , může-li matice B vzniknout z A pomocí konečného počtu elementárních transformací. Zapisujeme jako $A \sim B$.

Příklad 2.13. Ověřte, zda jsou matice A a B řádkově ekvivalentní, je-li

$$A = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 2 & 3 & -2 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 3 & -6 & 0 \end{pmatrix}.$$

K druhému řádku matice A přičteme (-2) -násobek řádku prvního.

$$A = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 2 & 3 & -2 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 3 & -6 & 0 \end{pmatrix} = B$$

Pokud bychom vykonali řádkovou elementární úpravu na matici B , která je opačná k předchozí operaci, tj. přičteme 2-násobek prvního řádku k řádku druhému, platí

$$B = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 3 & -6 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 2 & 1 \\ 2 & 3 & -2 & 2 \end{pmatrix} = A$$

3 DETERMINANTY

Jako determinant chápeme číslo, které určitým způsobem charakterizuje čtvercové matice. Determinant se z definice počítá poměrně složitě a než bude zavedena samotná definice je nutností zmínit pojem permutace.

3.1 Permutace

Definice 3.1. Je-li konečná množina $A = \{a_1, a_2, \dots, a_n\}$, kde $n \geq 1$ tak pořadím π množiny A nazveme libovolnou posloupnost $\pi = (a_{k_1}, a_{k_2}, \dots, a_{k_n})$ takovou, že každý prvek z A je v ní zastoupen právě jednou.

Věta 3.1. Pro každou n -prvkovou množinu pro kterou platí $n \geq 1$ existuje právě $n!$ pořadí.

Definice 3.2. Základním pořadím na množině $A = \{1, 2, \dots, n\}$ rozumíme pořadí $\pi = \{1, 2, \dots, n\}$. Permutací na množině A rozumíme každou bijekci A na A a je-li permutace P množiny A , pak ji můžeme zapisovat ve tvaru

$$P = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ P(a_1) & P(a_2) & \dots & P(a_n) \end{pmatrix}.$$

Tedy permutaci je možno zapsat pomocí dvou pořadí, které se stručně zapisují jako

$$P = \begin{pmatrix} \pi_1 \\ \pi_2 \end{pmatrix}.$$

Pokud je π_1 seřazeno v základním pořadí $1, 2, \dots, n$ tak se zpravidla nepíše.

Příklad 3.1.

$$P = \begin{pmatrix} 2 & 1 & 3 & 5 & 4 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 5 & 4 & 1 & 2 \\ 5 & 4 & 2 & 1 & 3 \end{pmatrix}$$

jsou dva zápisy téže permutace P na množině $\{1, 2, 3, 4, 5\}$.

Věta 3.2. Pro každou n -prvkovou množinu pro kterou platí $n \geq 1$ existuje právě $n!$ permutací.

Příklad 3.2. Najděte v programu Wolfram Mathematica všechny čtyřprvkové permutace množiny A , je-li

$$A = \{1, 2, 3, 4\}$$

a zjistěte poté jaký je celkový počet jednotlivých permutací pomocí Věty 3.2.

```

1 In[38] := Permutations[{1, 2, 3, 4}, {4}]
2 Out[38] = {{1, 2, 3, 4}, {1, 2, 4, 3}, {1, 3, 2, 4}, {1, 3, 4, 2}, {1, 4, 2, 3},
3           {1, 4, 3, 2}, {2, 1, 3, 4}, {2, 1, 4, 3}, {2, 3, 1, 4}, {2, 3, 4, 1},
4           {2, 4, 1, 3}, {2, 4, 3, 1}, {3, 1, 2, 4}, {3, 1, 4, 2}, {3, 2, 1, 4},
5           {3, 2, 4, 1}, {3, 4, 1, 2}, {3, 4, 2, 1}, {4, 1, 2, 3}, {4, 1, 3, 2},
6           {4, 2, 1, 3}, {4, 2, 3, 1}, {4, 3, 1, 2}, {4, 3, 2, 1}}
7 In[39] := 4!
8 Out[39] = 24

```

Zdrojový kód 16 Permutace

Definice 3.3. Je-li $\pi = (k_1, k_2, \dots, k_n)$ pořadí, pak prvky k_i a k_j tvoří v pořadí π inverzi, je-li splněno $i < j$ a $k_i > k_j$.

Příklad 3.3. V pořadí $\pi = (2, 3, 1, 5, 4)$ tvoří inverze dvojice prvků

$$(2, 1), (3, 1), (5, 4).$$

Počet inverzí v π se označuje jako $[\pi]$. Z předchozího příkladu je

$$[\pi] = 3.$$

Definice 3.4. Znaménkem pořadí π se rozumí číslo $\text{sgn } \pi = (-1)^{[\pi]}$. Je-li výsledná hodnota $\text{sgn } \pi = 1$, pak se pořadí π nazývá sudé a pokud je výsledná hodnota $\text{sgn } \pi = -1$ hovoříme o lichém pořadí.

Příklad 3.4. Pro pořadí $\pi = (4, 3, 2, 5, 1)$ platí $[\pi] = 7$, tedy $\text{sgn } \pi = (-1)^7 = -1$. Pořadí π je liché.

Definice 3.5. Znaménkem permutace

$$P = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ P(a_1) & P(a_2) & \dots & P(a_n) \end{pmatrix} = \begin{pmatrix} \pi_1 \\ \pi_2 \end{pmatrix}$$

rozumíme číslo $\text{sgn } P$ které je rovno $+1$ pokud je $\text{sgn } \pi_1 = \text{sgn } \pi_2$, a je rovno -1 pokud platí $\text{sgn } \pi_1 = -\text{sgn } \pi_2$.

Příklad 3.5. Zjistěte jaké znaménko má následující permutace

$$P = \begin{pmatrix} 4 & 1 & 2 & 5 & 3 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix} = \begin{pmatrix} \pi_1 \\ \pi_2 \end{pmatrix}$$

Hodnota $[\pi_1] = 4$ a hodnota $[\pi_2] = 6$, tj. $\text{sgn } \pi_1 = 1$, $\text{sgn } \pi_2 = 1$, z čehož $\text{sgn } \pi_1 = \text{sgn } \pi_2$. Znaménko permutace P je tedy $+1$.

3.2 Determinant čtvercových matic

Determinantem rozumíme prvek, přiřazený čtvercové matici nad komutativním tělesem \mathcal{T} . Jinak můžeme determinant označit jako součet všech součinů prvků této matice takových, že v žádném z uvedených součinů se nevyskytují dva prvky z téhož řádku ani z téhož sloupce.

Každému součinu se přitom přiřazuje znaménko $+$ pokud jde o sudou permutaci a znaménko $-$ pokud se jedná o lichou permutaci.

Definice 3.6. Matice A stupně n nad tělesem \mathcal{T} se zapisuje

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}.$$

Determinantem této matice pak rozumíme prvek $\det A$ z tělesa \mathcal{T} takový, že

$$\det A = \sum_P \operatorname{sgn} P \cdot a_{1k_1} \cdot a_{2k_2} \cdot \dots \cdot a_{nk_n}$$

kde sčítáme přes všechny permutace

$$P = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ P(1) & P(2) & \dots & P(n) \end{pmatrix}$$

množiny $\{1, 2, \dots, n\}$.

Každý ze součinů $a_{1k_1} \cdot a_{2k_2} \cdot \dots \cdot a_{nk_n}$ se nazývá člen determinantu $\det A$.

Determinant matice A se také označuje jako $|A|$, popřípadě i jako

$$\det A = |A| = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

3.2.1 Vlastnosti determinantu

1. Má-li čtvercová matice v libovolném řádku nuly, pak je $\det A = 0$. Podle definice determinantu se v každém členu vyskytuje právě jeden prvek z i -tého řádku, musí být každý člen determinantu roven nule, což implikuje to, že je i celý determinant roven nule.

2. Má-li matice $A \in M_n(\mathcal{T})$ všechny prvky pod hlavní diagonálou rovny nule, pak je $\det A$ roven součinu $a_{11} \cdot a_{22} \cdot \dots \cdot a_{nn}$ prvků na hlavní diagonále.
3. Vznikne-li matice B ze čtvercové matice A stupně n záměnnou i -tého a j -tého řádku, kde $i \neq j$, potom $\det B = -\det A$.
4. Vznikne-li matice B vynásobením i -tého řádku matice $A \in M_n(\mathcal{T})$ prvkem $c \in \mathcal{T}$, pak platí $\det B = c \cdot \det A$.
5. Nechť $A \in M_n(\mathcal{T})$. Vznikne-li matice $B \in M_n(\mathcal{T})$ z matice A tak, že k libovolnému řádku matice A přičteme libovolnou lineární kombinaci ostatních řádků této matice, pak platí $\det B = \det A$.
6. Jsou-li řádkové vektory matice $A \in M_n(\mathcal{T})$ lineárně závislé, pak $\det A = 0$. Z čeho plyne, že jestliže se v matici $A \in M_n(\mathcal{T})$ rovnají i -tý a j -tý řádek, kde $i \neq j$, potom $\det A = 0$.
7. Pro každou čtvercovou matici $A \in M_n(\mathcal{T})$ platí $\det A^T = \det A$ což vlastně znamená, že například místo řádků matic u elementárních úprav lze také analogicky používat sloupce matic.

3.3 Výpočet determinantů

3.3.1 Determinant matice 1. stupně

Čtvercová matice prvního stupně má pouze jeden řádek a jeden sloupec a je tedy zřejmé, že obsahuje pouze jednu hodnotu, která je zároveň i determinantem. Platí-li, že je matice stupně 1, tj. $A = (a_{11})$, pak je $\det A = a_{11}$.

V praxi se ale tento typ matic téměř nepoužívá, jelikož se v případě číselných matic jedná přímo o klasická čísla.

Příklad 3.6. Je-li

$$A = (3)$$

pak $\det A = 3$.

3.3.2 Determinant matice 2. stupně

Matice druhého stupně je definována jako

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Členy determinantu $\det A$ jsou součiny $a_{11} \cdot a_{22}$ a $a_{12} \cdot a_{21}$. Za pomoci permutací je možné zjistit znaménka těchto součinů a to tak, že

$$\operatorname{sgn} \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = 1, \quad \operatorname{sgn} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = -1$$

Výslednou hodnotou je tedy $\det A = a_{11} \cdot a_{22} - a_{12} \cdot a_{21}$.

Příklad 3.7. Určete determinant matice A , když

$$\operatorname{sgn} \begin{pmatrix} 3 & 2 \\ 4 & 5 \end{pmatrix}.$$

$$\det A = 3 \cdot 5 - 2 \cdot 4 = 7.$$

3.3.3 Determinant matice 3. stupně

Matice třetího stupně je definována jako

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

Podle definice permutace je opět možné zjistit počet členů determinantu a jejich znaménka. Těch je tedy celkově $3! = 6$.

$$\begin{aligned} P &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, & \operatorname{sgn} \pi &= +1, & \text{člen determinantu } a_{11} \cdot a_{22} \cdot a_{33} \\ P &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, & \operatorname{sgn} \pi &= +1, & \text{člen determinantu } a_{12} \cdot a_{23} \cdot a_{31} \\ P &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, & \operatorname{sgn} \pi &= +1, & \text{člen determinantu } a_{13} \cdot a_{21} \cdot a_{32} \\ P &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, & \operatorname{sgn} \pi &= -1, & \text{člen determinantu } a_{13} \cdot a_{22} \cdot a_{31} \\ P &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, & \operatorname{sgn} \pi &= -1, & \text{člen determinantu } a_{12} \cdot a_{21} \cdot a_{33} \\ P &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, & \operatorname{sgn} \pi &= -1, & \text{člen determinantu } a_{11} \cdot a_{23} \cdot a_{32} \end{aligned}$$

Platí tedy

$$\det A = a_{11} \cdot a_{22} \cdot a_{33} + a_{12} \cdot a_{23} \cdot a_{31} + a_{13} \cdot a_{21} \cdot a_{32} - a_{13} \cdot a_{21} \cdot a_{33} - a_{12} \cdot a_{23} \cdot a_{31} - a_{11} \cdot a_{21} \cdot a_{32}.$$

Tento vzorec je jednodušejší zapamatovatelný pomocí následujícího pravidla. Jako první krok je nutné provést opis prvního a druhého řádku matice pod prvky a_{31}, a_{32}, a_{33} původní matice. Nejprve se násobí prvky na hlavní diagonále, dále ve směrech rovnoběžných s diagonálou. Součiny postupně sčítáme. Poté se násobí prvky na vedlejší diagonále. Vedlejší diagonálou rozumíme prvky a_{ij} , pro které platí $i = 1, \dots, n; j = n + 1 - i$. Dále ve směrech rovnoběžných s vedlejší diagonálou, přičemž v tomto případě se součiny odečítají. Tato mnemotechnická pomůcka se nazývá Sarussovo pravidlo a slouží pouze k lepšímu zapamatování postupu výpočtu determinantu matic 3. stupně.

Příklad 3.8. Určete determinant matice 3. stupně, když

$$A = \begin{pmatrix} 1 & -3 & -4 \\ -3 & 3 & -13 \\ -2 & 9 & 1 \end{pmatrix}.$$

Dle Sarussova pravidla

$$\det A = \begin{vmatrix} 1 & -3 & -4 \\ -3 & 3 & -13 \\ -2 & 9 & 1 \end{vmatrix} = 3 + 108 - 78 - 24 + 117 - 9 = 117.$$

3.3.4 Determinant matice 4. stupně

U matic stupně čtyři a více, je už nutné rozložit determinant na subdeterminanty nižšího řádu.

Definice 3.7. Necht $A = (a_{ij})$ je matice stupně $m \times n$. Potom se každá matice, která vznikne z matice A vynecháním některých řádků, či sloupců nazývá dílčí matice A . Je-li dílčí matice matice A čtvercová, jejím determinatem je subdeterminant matice A .

Definice 3.8. Je-li $A = (a_{ij}) \in M_n(\mathcal{T})$, potom se subdeterminant dílčí matice A_{ij} stupně $n - 1$ vzniklé vynecháním i -tého řádku a j -tého sloupce nazývá minor matice A příslušný k prvku a_{ij} a značí se \mathcal{M}_{ij} .

Algebraickým doplňkem prvku a_{ij} rozumíme $\mathcal{A}_{ij} = (-1)^{i+j} \mathcal{M}_{ij}$.

Příklad 3.9. Jaká je hodnota algebraického doplňku \mathcal{A}_{13} matice

$$A = \begin{pmatrix} 1 & 2 & 4 \\ 2 & -4 & 5 \\ -3 & 9 & -5 \end{pmatrix}.$$

Pro minor této matice platí $\mathcal{M}_{13} = 18 - 12 = 6$, kdy $\mathcal{A}_{13} = (-1)^{1+3} \cdot 6 = 6$. Algebraický doplňek \mathcal{A}_{13} je roven 6.

Věta 3.3. (Laplaceova věta) Nechť $A = (a_{ik}) \in M_n(\mathcal{T})$. Pak

- pro každé $i = 1, \dots, n$ platí

$$\sum_{k=1}^n a_{ik} \mathcal{A}_{ik} = \det A$$

- pro každé $i, j = 1, \dots, n, i \neq j$ platí

$$\sum_{k=1}^n a_{ik} \mathcal{A}_{jk} = 0.$$

Příklad 3.10. Vypočítejte hodnotu determinantu matice

$$A = \begin{pmatrix} 6 & -2 & 1 & 1 \\ 2 & -3 & 2 & -1 \\ 0 & 4 & 0 & 0 \\ 1 & 3 & 1 & 2 \end{pmatrix}.$$

V případě výpočtu determinantu matice vyššího řádu je výhodné využít vlastnosti determinantu. Proto v tomto případě bude nejvýhodnější rozvinout determinant podle 3. řádku, jelikož obsahuje jenom jeden nenulový prvek. Vynecháváme tedy 3. řádek a 2. sloupec.

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

$$-4 \cdot [24 - 1 + 2 - (2 - 6 + 4)] = -4 \cdot 25 = -100.$$

Příklad 3.11. Vypočítejte determinant matice

$$A = \begin{pmatrix} -2 & 4 & -2 & 6 \\ 1 & 9 & 1 & 2 \\ 2 & 0 & 2 & 1 \\ -3 & 15 & -3 & 6 \end{pmatrix}.$$

V případě tohoto příkladu není třeba provádět rozvoj, jelikož se v 1. a 3. sloupci nachází totožné hodnoty a tím pádem jsou sloupce lineárně závislé. Vzhledem k vlastnostem determinantu je tedy

$$\begin{vmatrix} -2 & 4 & -2 & 6 \\ 1 & 9 & 1 & 2 \\ 2 & 0 & 2 & 1 \\ -3 & 15 & -3 & 6 \end{vmatrix} = 0.$$

Příklad 3.12. Vypočítejte v program Wolfram Mathematica determinant matice

$$B = \begin{pmatrix} 2 & 1 & 0 & 5 & 9 \\ 1 & 0 & 0 & 6 & 6 \\ 0 & 2 & 3 & 9 & 0 \\ 1 & 0 & 3 & 8 & 1 \\ 2 & 1 & 1 & 11 & 2 \end{pmatrix}$$

```

1 In[40]:=B={{2,1,0,5,9},{1,0,0,6,6},{0,2,3,9,0},{1,0,3,8,1},
2           {2,1,1,11,2}};
3
4 In[41]:= Det[B]
5 Out[41]= -512

```

Zdrojový kód 17 Výpočet determinantu

3.4 Inverzní matice

Definice 3.9. Čtvercová matice A řádu n se nazývá regulární, když je tvořena lineárně nezávislými řádky. Čtvercová matice A řádu n se nazývá singulární, jestliže není regulární, tj. obsahuje řádky, které jsou lineárně závislé.

Definice 3.10. Je-li čtvercová matice A řádu n pak se matice B nazývá *inverzní matice* k matici A jestliže

$$AB = BA = E.$$

kde E je jednotková matice.

Věta 3.4. Nechť A je čtvercová matice řádu n . Pak k matici A existuje inverzní matice právě tehdy, když A je regulární. Inverzní matice k matici A je určena jednoznačně. Inverzní matice k regulární matici A se značí symbolem A^{-1} .

Věta 3.5. 1. Platí-li pro matice A, B vztah $AB = E$, pak také $BA = E$ a $A = B^{-1}$, $B = A^{-1}$.

2. Pro determinant inverzní matice k regulární matici A platí

$$\det A^{-1} = \frac{1}{\det A}.$$

3. Buď A regulární matice. Pak A^{-1} je regulární a platí

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

4. Pro libovolné regulární matice A, B platí

$$(AB)^{-1} = B^{-1}A^{-1}.$$

5. Je-li A regulární matice a B matice taková, že $AB = 0$, pak $B = 0$.

6. Je-li A regulární matice a B matice taková, že $AB = A$ nebo $BA = A$, pak $B = E$.

Věta 3.6. Má-li inverzní matice A^{-1} prvky a_{ij} , kde i je řádek matice a j je sloupec matice, pak

$$a_{ij} = \frac{(-1)^{i+j} \cdot \mathcal{M}_{ji}}{\det A},$$

kde \mathcal{M}_{ji} je subdeterminant matice A , který vznikl vynecháním j -tého řádku a i -tého sloupce.

Příklad 3.13. Vypočítejte inverzní matici k matici

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

K řešení toho typu příkladu lze použít řádkové elementární transformace uvedené v Definici 2.14. Napravo vedle matice A se připsá jednotková matice a na tuto nově vzniklou matici $A|E \in M_{2 \times 4}(\mathcal{T})$ aplikujeme konečný počet řádkových elementárních transformací takových, že se pozice jednotkové matice posune na levou stranu. Na pravé straně bude matice inverzní.

$$\left(\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 4 & 3 & 0 & 1 \end{array} \right)$$

První řádkovou úpravou bude vynásobení prvního řádku matice číslem (-2) a následné přičtení k řádku druhému. Dostáváme tedy

$$\left(\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 0 & 1 & -2 & 1 \end{array} \right)$$

Druhou řádkovou úpravou bude vynásobení druhého řádku matice číslem (-1) a přičtení k řádku prvnímu.

$$\left(\begin{array}{cc|cc} 2 & 0 & 3 & -1 \\ 0 & 1 & -2 & 1 \end{array} \right)$$

Posledním krokem bude vydělení prvního řádku číslem 2 a po této operaci dostáváme řešení tohoto příkladu

$$\left(\begin{array}{cc|cc} 1 & 0 & \frac{3}{2} & -\frac{1}{2} \\ 0 & 1 & -2 & 1 \end{array} \right)$$

Inverzní matice matice A je tedy

$$\begin{pmatrix} \frac{3}{2} & -\frac{1}{2} \\ -2 & 1 \end{pmatrix}$$

Příklad 3.14. Vypočítejte inverzní matici k matici A za pomoci subdeterminantů z Věty 3.6.

$$A = \begin{pmatrix} 3 & 4 \\ 7 & 8 \end{pmatrix}$$

Pro prvek a_{11}^{-1} inverzní matice A^{-1} platí

$$a_{11}^{-1} = \frac{(-1)^{1+1} \cdot 8}{-4} = -2$$

Pro prvek a_{12}^{-1} inverzní matice A^{-1} platí

$$a_{12}^{-1} = \frac{(-1)^{1+2} \cdot 7}{-4} = \frac{7}{4}$$

Pro prvek a_{21}^{-1} inverzní matice A^{-1} platí

$$a_{21}^{-1} = \frac{(-1)^{2+1} \cdot 4}{-4} = 1$$

Pro prvek a_{22}^{-1} inverzní matice A^{-1} platí

$$a_{22}^{-1} = \frac{(-1)^{2+2} \cdot 3}{-4} = -\frac{3}{4}$$

Výsledná inverzní matice má tedy tvar

$$A = \begin{pmatrix} -2 & 1 \\ \frac{7}{4} & -\frac{3}{4} \end{pmatrix}$$

Příklad 3.15. Najděte inverzní matici k matici A v programu Wolfram Mathematica je-li

$$A = \begin{pmatrix} 3 & -4 & 5 & 10 \\ 2 & -3 & 1 & 9 \\ 3 & -5 & -1 & 7 \\ 3 & -4 & 5 & 15 \end{pmatrix}$$

```
1 In[18]:= A = {{3,-4,5,10}, {2,-3,1,9}, {3,-5,-1,7},  
2           {3,-4,5,15}};  
3  
4 In[19]:= MatrixForm[Inverse[A]]  
5  
6 Out[34]= 
$$\begin{pmatrix} \frac{64}{5} & 29 & -11 & -\frac{104}{5} \\ \frac{38}{5} & 18 & -7 & -\frac{63}{5} \\ -1 & -3 & 1 & 2 \\ -\frac{1}{5} & 0 & 0 & \frac{1}{5} \end{pmatrix}$$
  
7  
8  
9  
10
```

Zdrojový kód 18 Inverzní matice

4 SOUSTAVY LINEÁRNÍCH ROVNIC

4.1 Hodnost matice

Definice 4.1. Hodností matice $A \in M_{m \times n}(\mathcal{T})$ rozumíme počet prvků maximálního lineárně nezávislého systému řádků matice A . Hodnost matice A se značí jako $h(A)$.

Z výše uvedené definice tedy přímo vyplývá že

- Hodnost nulové matice je rovna 0
- Hodnost nenulové matice je ≥ 1
- Hodnost diagonální matice je rovna počtu nenulových řádků.

Věta 4.1. Čtvercová matice A stupně n je regulární, je-li $h(A) = n$ (tedy je tvořena lineárně nezávislými řádky). Čtvercová matice A stupně n je singulární je-li $h(A) < n$.

Všechny řádkově ekvivalentní matice mají stejnou hodnost. Jinak řečeno, je možné použít konečné množství řádkových elementárních úprav a hodnost matice zůstane pořád stejná.

Příklad 4.1. Určete hodnost matice A pomocí elementárních řádkových transformací.

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

Prvním krokem bude výměna druhého řádku a prvního řádku. Tím dosáhneme toho, že bude prvek $a_{11} = 1$, což výrazně usnadní další úpravy. K druhému řádku poté přičteme první řádek vynásobený číslem (-2) a ke třetímu řádku přičteme první řádek vynásobený číslem (-1) . Poslední úpravou bude přičtení druhého řádku vynásobeného číslem 2 k řádku třetímu.

$$A = \begin{pmatrix} 2 & 2 & 1 \\ 1 & 2 & -1 \\ 1 & 6 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & -1 \\ 2 & 2 & 1 \\ 1 & 6 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & -1 \\ 0 & -2 & -3 \\ 0 & 4 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & -1 \\ 0 & -2 & -3 \\ 0 & 0 & 10 \end{pmatrix}$$

Získali jsme matici, která má všechny prvky na hlavní diagonále nenulové. Tedy tato matice má (a tedy i matice původní) hodnost 3.

Věta 4.2. Hodnost matice A je rovna maximálnímu stupni nenulového subdeterminantu matice A .

Příklad 4.2. Určete hodnotu matice A pomocí subdeterminantů (minorů).

$$A = \begin{pmatrix} 2 & -2 & 1 & 8 & 2 \\ 5 & -3 & 5 & 1 & 6 \\ -1 & 1 & 3 & 2 & -3 \end{pmatrix}$$

Vybereme například čtvercový subdeterminant 2. stupně obsahující prvek $a_{11} = 2$

$$\mathcal{M} = \begin{vmatrix} 2 & -2 \\ 5 & -3 \end{vmatrix} = 4.$$

Tedy $h(A) \geq 2$. Dále vybereme čtvercové subdeterminanty 3. stupně

$$\begin{vmatrix} 2 & -2 & 1 \\ 5 & -3 & 5 \\ -1 & 1 & 3 \end{vmatrix} \quad \text{a} \quad \begin{vmatrix} 2 & -2 & 8 \\ 5 & -3 & 1 \\ -1 & 1 & 2 \end{vmatrix}$$

Protože jsou oba tyto subdeterminanty nenulové, platí $h(A) = 3$.

4.2 Řešení soustav lineárních rovnic

Definice 4.2. Soustavou m lineárních rovnic o n neznámých nad tělesem \mathcal{T} rozumíme soustavu ve tvaru

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= b_m \end{aligned}$$

kde $a_{ij} \in T$ jsou koeficienty soustavy rovnic, x_1, \dots, x_n jsou neznámé. Prvky $b_i \in T$, kde $i = 1, 2, \dots, m$, jsou absolutní členy soustavy nebo také pravá strana soustavy. Pokud platí $b_i = 0$ pro každé $i = 1, 2, \dots, m$, pak se soustava nazývá homogenní. V opačném případě se nazývá nehomogenní.

Uvedený systém lineárních rovnic lze stručněji zapsat i jako:

$$\sum_{j=1}^n a_{ij}x_j = b_i, \quad 1 \leq i \leq m$$

Definice 4.3. Uvažujeme-li soustavu rovnic z předchozí definice, potom matici

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, \quad \text{resp. } A|b = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{array} \right)$$

nazýváme maticí soustavy lineárních rovnic, resp. rozšířenou maticí soustavy lineárních rovnic.

Označíme-li

$$\vec{x}^T = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \text{ a } \vec{b}^T = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix},$$

Pak soustavu lineárních rovnic můžeme zapsat ve tvaru

$$A\vec{x}^T = \vec{b}^T.$$

Definice 4.4. Uvažujeme dva systémy lineárních rovnic $A\vec{x} = \vec{b}$, $B\vec{y} = \vec{c}$. Řekneme, že tyto systémy jsou ekvivalentní a píšeme $A\vec{x} = \vec{b} \sim B\vec{y} = \vec{c}$, jestliže množina všech řešení systému $A\vec{x} = \vec{b}$ splývá s množinou všech řešení systému $B\vec{y} = \vec{c}$.

Ekvivalentní systémy rovnic musí mít stejný počet neznámých x_1, \dots, x_n , ale mohou se lišit počtem rovnic.

Definice 4.5. Soustava lineárních rovnic $A\vec{x} = \vec{b}$ se nazývá řešitelná, pokud existuje alespoň jedno její řešení.

Věta 4.3. (Frobeniova věta) Systém m lineárních rovnic o n neznámých $A\vec{x} = \vec{b}$ má řešení právě tehdy, když hodnota matice A je rovna hodnotě matice rozšířené $(A|b)$.

Věta 4.4. Jsou-li $A\vec{x} = \vec{b}$ a $B\vec{y} = \vec{c}$ dvě soustavy nehomogenních lineárních rovnic o n neznámých takové, že jejich rozšířené matice $(A|b)$ a $(B|c)$ jsou řádkově ekvivalentní, pak jsou tyto soustavy ekvivalentní.

Na základě předešlé věty je založena také metoda řešení soustav lineárních rovnic zvaná **Gaussova eliminační metoda**. Tato metoda spočívá v aplikaci řádkových elementárních úprav na rozšířenou matici soustavy tak, aby se pod hlavní diagonálou této matice nacházely pouze nuly. Takto upravená matice odpovídá soustavě rovnic, která je ekvivalentní se soustavou původní.

Příklad 4.3. Řešte zadanou soustavu rovnic v prostředí Wolfram Mathematica.

$$x_1 + 2x_2 + 3x_3 = 14$$

$$3x_1 + 2x_2 + x_3 = 10$$

$$3x_1 + x_2 + 2x_3 = 11$$

```

1 In[4] := Solve[{x1+2x2+3x3==14, 3x1+2x2+x3==10, 3x1+x2+2x3==11},
2           {x1, x2, x3}]
3 Out[4] = {{x1->1, x2->2, x3->3}}
```

Zdrojový kód 19 Řešení soustavy rovnic

Výstupem programu jsou nalezené hodnoty řešení soustavy rovnic $x_1 = 1, x_2 = 2, x_3 = 3$.

Příklad 4.4. Řešte následující systém rovnic pomocí Gaussovy eliminační metody.

$$x_1 + 4x_2 - x_3 = 6$$

$$2x_1 + 3x_2 + x_3 = 2$$

$$3x_1 + 7x_2 + 2x_3 = 18$$

Prvním krokem bude přepsání soustavy rovnic do tvaru odpovídající rozšířené matice.

$$\left(\begin{array}{ccc|c} 1 & 4 & -1 & 6 \\ 2 & 3 & 1 & 2 \\ 3 & 7 & 2 & 18 \end{array} \right)$$

Nyní se je potřeba upravit matici pomocí elementárních transformací tak abychom dosáhli tzv. *schodovitého tvaru* matice. Matice je ve schodovitém tvaru, jestliže případné nulové řádky jsou uspořádány na konci matice a nenulové řádky jsou uspořádány tak, že každý následující řádek začíná větším počtem nul než řádek předchozí. Vynásobíme tedy 1. řádek číslem (-2) a přičteme k 2. řádku. Opět vynásobíme 1. řádek, ale v tomto případě číslem (-3) a přičteme k 3. řádku.

$$\left(\begin{array}{ccc|c} 1 & 4 & -1 & 6 \\ 0 & -5 & 3 & -10 \\ 0 & -5 & 5 & 0 \end{array} \right)$$

V posledním kroku stačí vynásobit 2. řádek číslem (-1) a přičíst k 3. řádku matice.

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

Z posledního řádku matice dostáváme rovnici

$$2x_3 = 10$$

$$x_3 = 5$$

Po dosazení hodnoty x_3 do druhého řádku soustavy rovnic dostáváme

$$-5x_2 + 3x_3 = -10$$

$$-5x_2 + 3 \cdot 5 = -10$$

$$-5x_2 = -25$$

$$x_2 = 5$$

Zbývá už jen dosadit hodnoty x_2 a x_3 do prvního řádku rovnice která je ve tvaru

$$x_1 + 4x_2 - x_3 = 6$$

$$x_1 + 4 \cdot 5 - 5 = 6$$

$$x_1 = -9$$

Z poslední matice bylo jasné, že hodnota původní matice a hodnota rozšířené matice je 3, tedy soustava je řešitelná a jelikož má poslední matice stejný počet řádků jako počet neznámých, má zadaná soustava jediné řešení. Tím je $x_1 = -9, x_2 = 5, x_3 = 5$.

Příklad 4.5. Vyřešte následující systém rovnic pomocí Gaussovy eliminační metody v programu Wolfram Mathematica.

$$8x_1 - x_2 - 2x_3 = 0$$

$$-x_1 + 7x_2 - x_3 = 10$$

$$-2x_1 - x_2 + 9x_3 = 23$$

```

1 In[1] := A = {{8,-1,-2,0}, {-1,7,-1,10}, {-2,-1,9,23}}
2 Out[1]= {{8,-1,-2,0}, {-1,7,-1,10}, {-2,-1,9,23}}
3
4 In[2] := RowReduce[A]
5 Out[2]= {{1,0,0,1}, {0,1,0,2}, {0,0,1,3}}
6
7 In[3] := MatrixForm[%]
8 Out[34]= 
$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{pmatrix}$$

9
10
11
```

Zdrojový kód 20 Gaussova eliminační metoda

Výstupem programu je redukovaná matice jejíž obsah lze po přepsání do soustavy lineárních rovnic interpretovat jako:

$$x_1 = 1, x_2 = 2, x_3 = 3.$$

Věta 4.5. (Cramerovo pravidlo) Necht' $A\vec{x} = \vec{b}$ je soustava n lineárních rovnic o n neznámých ($n \geq 1$) taková, že $\det A \neq 0$. Potom pro každé $j = 1, \dots, n$ platí

$$x_j = \frac{\det A_j}{\det A}.$$

Kde A_j je matice, která vznikne z A nahrazením j -tého sloupce vektorem \vec{b} .

Příklad 4.6. Následující systém rovnic řešte Cramerovým pravidlem

$$\begin{aligned} 2x_1 + 2x_2 - x_3 + x_4 &= 4 \\ 4x_1 + 3x_2 - x_3 + 2x_4 &= 6 \\ 8x_1 + 5x_2 - 3x_3 + 4x_4 &= 12 \\ 3x_1 + 3x_2 - 2x_3 + 2x_4 &= 6 \end{aligned}$$

Výpočet zahájíme přepisem soustavy rovnic do maticového tvaru.

$$A = \begin{pmatrix} 2 & 2 & -1 & 1 \\ 4 & 3 & -1 & 2 \\ 8 & 5 & -3 & 4 \\ 3 & 3 & -2 & 2 \end{pmatrix}$$

Determinant této matice je roven 2, takže je možné aplikovat Cramerovo pravidlo. Je-li se v zadání nachází 4 neznámé, musíme vytvořit 4 nové matice z matice původní, u kterých bude sloupec počítané neznámé nahrazen sloupcem hodnot pravé strany rovnice.

Pro x_1 :

$$A_1 = \begin{pmatrix} 4 & 2 & -1 & 1 \\ 6 & 3 & -1 & 2 \\ 12 & 5 & -3 & 4 \\ 6 & 3 & -2 & 2 \end{pmatrix}$$

Determinant této matice je roven 2, tedy platí $x_1 = \frac{2}{2} = 1$.

Pro x_2 :

$$A_2 = \begin{pmatrix} 2 & 4 & -1 & 1 \\ 4 & 6 & -1 & 2 \\ 8 & 12 & -3 & 4 \\ 3 & 6 & -2 & 2 \end{pmatrix}$$

Determinant této matice je roven 2, tedy platí $x_2 = \frac{2}{2} = 1$.

Pro x_3 :

$$A_3 = \begin{pmatrix} 2 & 2 & 4 & 1 \\ 4 & 3 & 6 & 2 \\ 8 & 5 & 12 & 4 \\ 3 & 3 & 6 & 2 \end{pmatrix}$$

Determinant této matice je roven -2 , tedy platí $x_3 = \frac{-2}{2} = -1$.

Pro x_4 :

$$A_4 = \begin{pmatrix} 2 & 2 & -1 & 4 \\ 4 & 3 & -1 & 6 \\ 8 & 5 & -3 & 12 \\ 3 & 3 & -2 & 6 \end{pmatrix}$$

Determinant této matice je roven -2 , tedy platí $x_4 = \frac{-2}{2} = -1$.

Příklad 4.7. Aplikujte Cramerovo pravidlo v prostředí Wolfram Mathematica pomocí jednoduché funkce, je-li:

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

tedy rozšířená matice soustavy je

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

```
1 In[13]:= A = {{1, 2, -1}, {-2, 1, -3}, {0, 2, -1}};  
2         b = {1, 2, -2};  
3  
4 In[15]:= VypocetX[x_, matice_, vektor_] :=  
5         Module[{detA, detAx, B},  
6         B = matice;  
7         B[[All, x]] = vektor;  
8         detAx = Det[B];  
9         detA = Det[matice];  
10        Return[  
11            detAx/detA]  
12  
13 In[16]:= {x_1 -> VypocetX[1, A, b],  
14         x_2 -> VypocetX[2, A, b],  
15         x_3 -> VypocetX[3, A, b]}  
16  
17 Out[16]= {x_1 -> 3, x_2 -> -(14/5), x_3 -> -(18/5)}
```

Zdrojový kód 21 Cramerovo pravidlo

5 VYUŽITÍ LINEÁRNÍ ALGEBRY V PRAXI

5.1 Šifrování

Šifrování využívá z lineární algebry teorii matic a jejich vlastnosti, které jsou pro tyto účely velice vhodné. Nejvýznamnějším způsobem je substituční Hillova šifra, která se hojně využívá v klasické kryptografii. Využívá lineární transformace bloku kódované zprávy za pomoci násobení matic.

Používaná abeceda může být například anglického typu využívající písmena A-Z bez diakritiky. V případě českého jazyka můžeme využít i diakritiku a pokud to okolnosti vyžadují, je možné využít i interpunkční znaménka. Každé písmeno, či znak je reprezentováno libovolným číslem v rozmezí rozsahu používané abecedy. V případě anglického typu by byly jednotlivé znaky reprezentovány čísly v rozmezí 0-25.

Zprávou může být libovolný text, po kterém požadujeme zašifrování a následné dešifrování u příjemce zprávy. Kódovaná zpráva musí obsahovat pouze znaky definované abecedy. Znaky zprávy můžeme ukládat do matice.

Šifrovacím klíčem je matice, kterou použijeme na zakódování požadované zprávy. Tento klíč ale musí splňovat následující podmínky:

- Matice klíče je čtvercová stupně n a zároveň platí, že počet znaků zprávy je dělitelný n .
- Determinant matice klíče a počet znaků abecedy musí být nesoudělná čísla.
- Matice je regulární.

Dešifrovacím klíčem je matice inverzní k šifrovacímu klíči.

Samotné šifrování je reprezentováno maticovým násobením. Vytvořená matice z požadované zprávy se vynásobí s vhodně zvoleným šifrovacím klíčem. Na každý prvek matice vzniklé násobením se poté provede celočíselné dělení s počtem prvků abecedy. Výsledkem je zašifrovaná zpráva jak v číselné podobě, tak i v podobě textové.

Stejně znaky nejsou ale vždy reprezentovány stejným znakem v zašifrované podobě a to z toho důvodu, že Hillova šifra převádí celé m -tice znaků, a ne pouze každý jednotlivě. Proto není vůbec jednoduché tuto šifru prolomit.

Dešifrování zprávy probíhá na stejném principu jako šifrování. Zašifrovanou zprávu převedeme do číselné podoby a vepíšeme do matice. Matici následně vynásobíme inverzní

maticí klíče. Na výslednou matici opět aplikujeme celočíselné dělení počtem prvků abecedy.

Výsledná dešifrovaná zpráva je stejná, jako zpráva, která byla šifrována.

5.1.1 Hillova šifra v prostředí Wolfram Mathematica

Prvním krokem k vytvoření zašifrované zprávy je zvolení vhodné abecedy. Pro účely demonstrace kódu byla zvolena abeceda anglického typu obsahující pouze velká, malá písmena bez diakritiky, doplněné o interpunkční znaménka a mezeru. V druhém kroku dojde k uložení hodnoty délky zvolené abecedy do proměnné.

```

1 In[1]:= Abeceda =
2 "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ .? , ! ' - "
3 DelkaAbecedy = StringLength[Abeceda];
4 In[2]:= Zprava = " ";

```

Zdrojový kód 22 Vytvoření abecedy a zprávy

V následujícím kroku je nutné vytvořit matice klíče, který bude sloužit pro šifrování námi zvolené zprávy. Vytvořená matice je stupně n , pro $2 \leq n \leq 9$. Je nutné si dát pozor aby determinant těchto matic nebyl soudělný s počtem znaků zvolené abecedy. Pro byla zvolena abeceda o prvočíselné délce. Konkrétně 59 znaků.

```

1 In[2241]:= MatrixForm[Klic5]
2
3
4
5 Out[34]= 
$$\begin{pmatrix} 5 & -2 & -9 & -6 & -4 \\ -4 & -2 & 1 & -7 & -3 \\ -7 & 6 & -1 & -6 & -8 \\ 4 & 7 & -4 & 1 & -7 \\ 9 & 6 & -8 & 6 & 2 \end{pmatrix}$$

6
7

```

Zdrojový kód 23 Matice klíče

Po vytvoření matice klíče je nutné vytvořit klíč inverzní, který bude sloužit k dešifrování. Ten bude vytvořen po aplikaci funkce VytvorInverzi.

```

1 In[2241]:= VytvorInverzi[klic_] := Inverse[klic, Modulus ->
    DelkaAbecedy]
2 InverzniKlic = VytvorInverzi[Klic]
3
4      
$$\begin{pmatrix} 55 & 1 & -6 & 39 & 36 \\ 54 & 8 & 52 & 1 & 7 \\ 20 & 15 & 24 & 54 & 23 \\ 58 & 6 & 10 & 5 & 35 \\ 57 & 43 & 1 & 52 & 1 \end{pmatrix}$$

5 Out[34]=
6
7

```

Zdrojový kód 24 Inverzní klíč

Z výstupu funkce TvorbaAsociace je jasné, jaké číselná hodnota byla přiřazena jakému znaku abecedy.

Po vytvoření asociace následuje vytvoření jednotlivých funkcí, ze kterých se bude skládat funkce výsledná sloužící pro šifrování a dešifrování zprávy.

```

1 In[1875]:=
2 Asociace[abeceda_] := PositionIndex@Characters[abeceda] - 1
3 Tabulka = Asociace[Abeceda]
4
5 Out[1876]= <|"a"-> {0}, "b"-> {1}, "c"-> {2}, "d"-> {3},
6 "e" -> {4}, "f"-> {5}, "g"-> {6}, "h"-> {7}, "i"-> {8},
7 "j" -> {9}, "k"-> {10}, "l"-> {11}, "m"-> {12}, "n"-> {13},
8 "o" -> {14}, "p"-> {15}, "q"-> {16}, "r" -> {17}, "s"-> {18},
9 "t" -> {19}, "u"-> {20}, "v"-> {21}, "w"-> {22}, "x"-> {23},
10 "y" -> {24}, "z"-> {25}, "A"-> {26}, "B"-> {27}, "C"-> {28},
11 "D" -> {29}, "E"-> {30}, "F"-> {31}, "G"-> {32}, "H"-> {33},
12 "I" -> {34}, "J"-> {35}, "K"-> {36}, "L"-> {37}, "M"-> {38},
13 "N" -> {39}, "O"-> {40}, "P"-> {41}, "Q"-> {42}, "R"-> {43},
14 "S" -> {44}, "T"-> {45}, "U"-> {46}, "V"-> {47}, "W"-> {48},
15 "X" -> {49}, "Y"-> {50}, "Z"-> {51}, " " -> {52}, "." -> {53},
16 "? " -> {54}, "," -> {55}, "!" -> {56}, "'" -> {57}, "-" -> {58} |>

```

Zdrojový kód 25 Vytvoření asociace znaků s čísly

Funkce Add slouží k tomu, aby byl text doplněn o tolik znaků mezer, aby vyhovoval šifrovacímu klíči. Princip funkce stojí na celočíselném dělení. Výstupem je text již doplněný o znaky mezer.

```
1 Add[text_, klic_] :=  
2 Module[{Vydel, NewString},  
3 Vydel = Mod[StringLength[text], Length@klic];  
4 NewString = Table[" ", Length@klic - Vydel];  
5 StringJoin[text, NewString]]
```

Zdrojový kód 26 Funkce doplnění zprávy

Funkce ApplyKey slouží k převodu znaků textu do jeho odpovídající číselné podoby, podle již vytvořené tabulky. Výstupem této funkce je seznam čísel již zašifrovaného textu.

```
1 ApplyKey[doplnenytex_, kod_, klic_] :=  
2 Flatten[Mod[  
3 Partition[Map[Function[x, kod[x] [[1]]], Characters[  
    doplnenytex_]],  
4 Length@klic].klic, DelkaAbecedy]]
```

Zdrojový kód 27 Funkce aplikace šifrovacího klíče

Následující funkcí je funkce MakeText. Jejím účelem je převod zašifrovaného textu v číselné podobě zpět do formy znaků. Tento převod je umožněn pomocí vytvořených asociací z funkce Asociace. Výsledkem funkce MakeText je text v jeho zašifrované nebo dešifrované podobě.

```
1 MakeText[zasifrovanytext_, kod_] :=  
2 StringJoin[  
3 Flatten[Map[Function[x, PositionIndex [kod] [[x]]],  
4 zasifrovanytext + 1]]]
```

Zdrojový kód 28 Funkce převodu čísel na text

Funkce HillCiper byla vytvořena složením všech výše uvedených funkcí, které na sebe logicky navazují. Slouží jak pro šifrování textu, tak i pro jeho dešifrování.

```
1 HillCiper[text_, kod_, klic_] :=
2 MakeText[ApplyKey[Add[text, klic], kod, klic], kod]
```

Zdrojový kód 29 Funkce Hillova šifrování

5.1.2 Demonstrace Hillovy šifry na příkladu

Pro demonstraci funkčnosti zdrojového kódu uvedeného v předchozí podkapitole byl vybrán text, po kterém se požaduje zakódování, úryvek z knihy Pán prstenů od spisovatele J.R.R.Tolkiena[13].

```
1 Abeceda =
2 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ. !, '-';
3
4 Text = 'Three Rings for the Elven-kings under the sky, Seven
      for the Dwarf-lords in their halls of stone, Nine for
      Mortal Men doomed to die, One for the Dark Lord on his
      dark throne in the Land of Mordor where the Shadows lie.
      One Ring to rule them all, One Ring to find them, One Ring
      to bring them all and in the darkness bind them in the
      Land of Mordor where the Shadows lie.';
```

Zdrojový kód 30 Zvolení abecedy a vložení textu

```
1 In[22]:= Cipher = HillCiper[Zprava, Tabulka, Klic]
2
3 Out [22]= "mYju!uS' LZ!FVBwDe!gYHGn.FfND,i'EED-wGHtVbHcmqxBL' .
      TRDq.SX!P,zn TJRWUBixYNRtUJ?LvTDOELpChmVZGumTsRQpFiR' zS!?
      xm'LEoPuLDLoickSfs?uk-Ziv'UITa,tDe!
      gYdnHUssMdlXbMOUoNUzsixpRYICyt!y'HgmoXyYjlsGrmnMYnP!ySLEMq
      ,bWdTrfxT.?iPSnaqpVLmBc!tdz-oyRpRxawcDopOwGv'ma'.J.S'
      dIcbLfQ!e.LrQFYVLmBc!tdz-YmDtKWmLWO?pW?KamJRh-GxRdi?YpBJ'
      kJRZs.xawcDSx pUNsKj A?HUzUP?wRzHXvTiVE-VmYl-rwT z!
      eGndjknDzw"
```

Zdrojový kód 31 Šifrování textu

```
1 In[23]:= Decipher = HillCipher[Cipher, Tabulka, InverzniKlic]
2
3 Out[23]= "Three Rings for the Elven-kings under the sky,
  Seven for the Dwarf-lords in their halls of stone, Nine
  for Mortal Men doomed to die, One for the Dark Lord on his
  dark throne in the Land of Mordor where the Shadows lie.
  One Ring to rule them all, One Ring to find them, One Ring
  to bring them all and in the darkness bind them in the
  Land of Mordor where the Shadows lie."
```

Zdrojový kód 32 Dešifrování textu

5.2 Geometrické transformace

Geometrické transformace se nejvíce používají v počítačové grafice. V této kapitole se budu zabývat transformacemi, které jsou lineární. Mezi ty se řadí například otáčení, posunutí, zkosení a nebo třeba změna měřítka. Objekty jsou reprezentovány souřadnicemi, které se váží k souřadnicovému systému. Geometrické transformace se aplikují na jednotlivé body neboli souřadnice objektu, který následně mění svoji velikost nebo polohu. S grafickou transformací objektu souvisí také transformace bodu P , který má v kartézské soustavě souřadnice $[X, Y]$. Transformací T , kterou aplikujeme na bod P dostáváme bod o souřadnicích $[X', Y']$. Transformací celého objektu rozumíme aplikaci transformace na všechny body, ze kterých se objekt skládá, nebo pokud to transformace dovoluje, tak pouze na parametry jasně určující objekt.

5.2.1 Homogenní souřadnice

Pro jednodušší výpočty transformací se využívá reprezentace bodů pomocí tzv. homogenních souřadnic. Tato reprezentace se používá z důvodu, že homogenní souřadnice umožňují aplikaci základních lineárních transformací pouze pomocí násobení matic, což v případě kartézských souřadnic, které jsou nehomogenní není možné. Skládání transformací se realizuje jako násobení matic a inverzní transformace je reprezentována pomocí inverzní matice. Nynější grafické procesory s jednoduchostí provádí výše uvedené maticové operace a rychlost zpracování scény se díky specializovaným grafickým kartám neustále zvyšuje. Uspořádaná trojice čísel $[x, y, w]$ představuje homogenní souřadnice bodu P s kartézskými souřadnicemi $[X, Y]$, platí-li:

$$X = \frac{x}{w}, \quad Y = \frac{y}{w}, \quad w \neq 0.$$

Bod P je svými homogenními souřadnicemi určen naprosto jednoznačně. Souřadnice w se též nazýváme *váhou bodu*. Homogenní souřadnice transformovaného bodu P' $[X', Y']$ se označují jako $[x', y', w']$. Často se volí $w = 1$, potom jsou tedy homogenní souřadnice bodu $[X, Y, 1]$. Obecnou čtvercovou matici stupně 3 reprezentující lineární transformaci bodu $P = [x, y, w]$ na bod $P' = [x', y', w']$ je matice A taková, že

$$P'^T = \begin{bmatrix} x' \\ y' \\ w' \end{bmatrix} = P \cdot A = \begin{bmatrix} x \\ y \\ w \end{bmatrix} \cdot \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}.$$

5.2.2 Dvourozměrné geometrické transformace

1. Posunutí

Transformace posunutí nebo také translace bodu P je určena vektorem posunutí $\vec{v} = (v_x, v_y)$.

Matice transformace posunutí T má tvar

$$T(v_x, v_y) = \begin{bmatrix} 1 & 0 & v_x \\ 0 & 1 & v_y \\ 0 & 0 & 1 \end{bmatrix}$$

2. Otočení

Otáčením, neboli rotací bodu P kolem počátku soustavy souřadnic $O = [0, 0]$ o úhel α získáme bod P' o souřadnicích

$$\begin{aligned} X' &= X \cos \alpha - Y \sin \alpha \\ Y' &= X \sin \alpha + Y \cos \alpha. \end{aligned}$$

Matice transformace otočení R má tvar

$$R(\alpha) = \begin{bmatrix} \cos \alpha & -\sin \alpha & 0 \\ \sin \alpha & \cos \alpha & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

3. Změna měřítka

Změna měřítka ovlivňuje velikost transformovaného objektu ve směru souřadnicových os. Pokud je absolutní hodnota koeficientu měřítkování v intervalu $(0, 1)$, dochází ke zmenšení a přiblížení transformovaného objektu k počátku souřadnic. Je-li absolutní hodnota koeficientu větší než jedna, dojde k prodloužení, je-li znaménko koeficientu záporné, dochází k prodloužení či zmenšení v opačném směru. Matice pro změnu měřítka S má tvar

$$S(s_x, s_y) = \begin{bmatrix} s_x & 0 & 0 \\ 0 & s_y & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

kde s_x je koeficient změny měřítka ve směru souřadnicové osy x a s_y je koeficient změny měřítka ve směru souřadnicové osy y .

4. Souměrnost

Souměrnost, neboli zrcadlení je zvláštním případem změny měřítka, kde se absolutní hodnota koeficientu měřítka rovna jedné. Souměrnost je možno ve dvourozměrném případě rozdělit na souměrnost středovou a osovou. Středová souměrnost podle počátku souřadnicové soustavy je otáčením o 180° resp. změnou měřítka $s_x = -1$ a $s_y = -1$, zatímco osové souměrnosti získáme překlopením bodu podle jedné ze souřadnicových os. Souměrnost podle osy x má koeficienty $s_x = -1$ a $s_y = 1$, obdobně pro osu y je $s_x = 1$ a $s_y = -1$.

Matice pro zrcadlení S mají tvar

$$Ref_0 = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad Ref_x = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad Ref_y = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

5. Zkosení

Transformace zkosení s koeficientem sh_x (z anglického shear) znamená zkosení ve směru osy x . Analogicky se provádí zkosení ve směru osy y s koeficientem sh_y .

Transformační matice Sh_x a Sh_y mají tvar

$$Sh_x = \begin{bmatrix} 1 & sh_x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad Sh_y = \begin{bmatrix} 1 & 0 & 0 \\ sh_y & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

5.2.3 Skládání transformací

Při aplikování transformací na body zvoleného objektu záleží na pořadí, v jakém se transformace provádějí. Je totiž rozdíl, jestliže bod posuneme a poté otočíme okolo počátku souřadnicového systému, nebo zda bod nejprve otočíme a poté provedeme posunutí. Transformaci vzniklou složením z více transformací lze vyjádřit jedinou maticí, již získáme násobením matic, reprezentujících dílčí transformace. Protože záleží na pořadí transformací, záleží také na pořadí násobení matic. Jestliže používáme zápis $P' = P.A$, musíme matice reprezentující následující transformace přidávat do této transformace zleva. Pokud tedy aplikujeme transformace v pořadí T_1, T_2 pak je bod P transformován vztahem $P' = T_2.T_1.P$.

5.2.4 Grafické transformace v programu Wolfram Mathematica

Před zahájením aplikace transformací na základní matici *Basic* je důležité si vhodně vytvořit funkce, které budou vytvářet body pro objekt z matice transformace a zároveň vykreslovat graf, který slouží k ilustraci a vizuálnímu ověření, zda transformace proběhla správně.

```

1 BodyObjektu[x_] := {
2     x1 = x[[1, 3]];
3     y1 = x[[2, 3]];
4     x2 = x[[1, 1]];
5     y2 = x[[2, 1]];
6     x3 = x[[1, 2]];
7     y3 = x[[2, 2]];
8
9     {x1, y1}, {x2, y2}, {x3, y3}}

```

Zdrojový kód 33 Funkce pro vytvoření bodů objektu

```

1 VykresliGraf[y_] :=
2 Graphics[{Thickness[0.01], Red,
3     Line[{{x1, y1}, {x2, y2}, {x3, y3}, {x1, y1}}],
4     Axes -> True, PlotRange -> 3, AxesLabel -> {Style["x"],
5         Style["y"]}}]

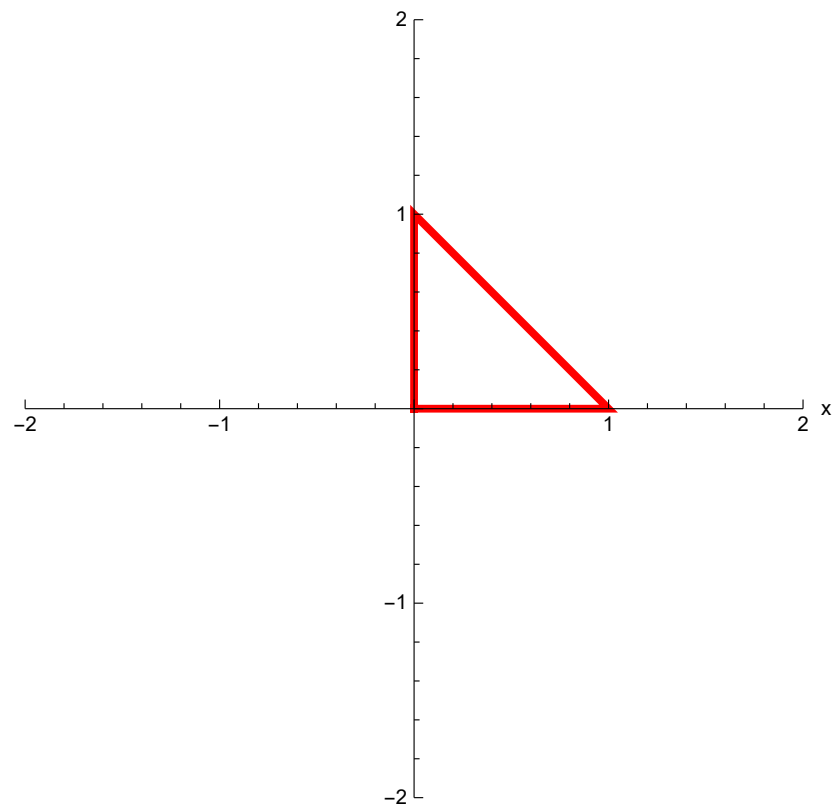
```

Zdrojový kód 34 Funkce pro vykreslení grafu objektu

1. Vytvoření základního objektu

```
1 In[95]:= Basic = {{1, 0, 0}, {0, 1, 0}, {1, 1, 1}};  
2 MatrixForm[Basic]  
3  
4      
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$
  
5 Out[34]=  
6  
7  
8 In[97]:= BodyObjektu[Basic]  
9 Out[97]= {{0, 0}, {1, 0}, {0, 1}}  
10  
11 In[98]:= VykresliGraf[Basic]
```

Zdrojový kód 35 Vytvoření základního objektu

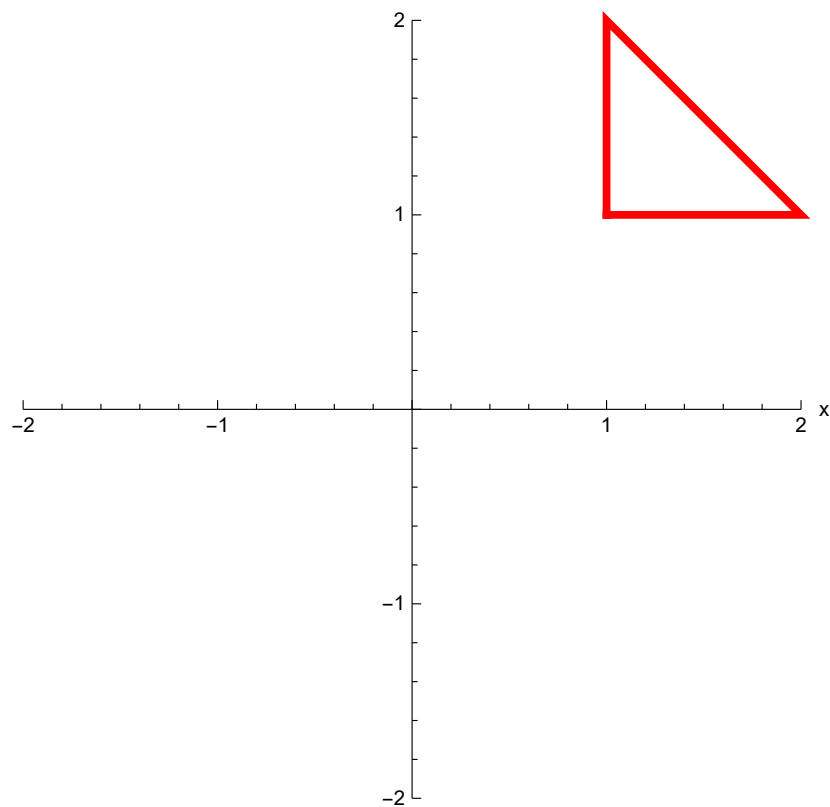


Obr. 1 Graf základního objektu

2. Transformace posunutí

```
1 In[14]:=TranslateM = {{1, 0, 1}, {0, 1, 1}, {0, 0, 1}};  
2 In[146]:= Translation = TranslateM.Basic;  
3 MatrixForm[TranslateM].MatrixForm[Basic]->  
4 MatrixForm[Translation]  
5  
6 Out[34]=  $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 1 \end{pmatrix}$   
7  
8  
9  
10 In[148]:= BodyObjektu[Translation]  
11 Out[148]= {{1, 1}, {2, 1}, {1, 2}}  
12  
13 In[149]:= VykresliGraf[Translation]
```

Zdrojový kód 36 Posunutí objektu

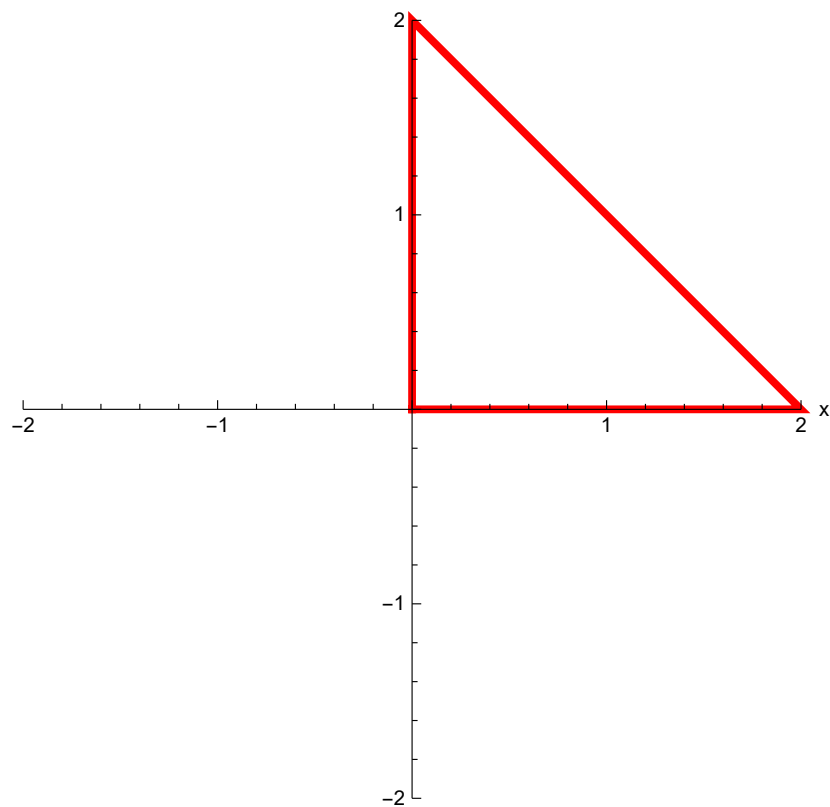


Obr. 2 Graf posunutí objektu

3. Transformace změny měřítka

```
1 In[566]:= ScaleM = {{2, 0, 0}, {0, 2, 0}, {0, 0, 1}};  
2 In[567]:= Scaling = ScaleMatrix.Basic;  
3 MatrixForm[ScaleM].MatrixForm[Basic] ->  
4 MatrixForm[Scaling]  
5  
6  
7 Out[34]=  $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix}$   
8  
9  
10 In[569]:= BodyObjektu[Scaling]  
11 Out[569]= {{0, 0}, {2, 0}, {0, 2}}  
12  
13 In[570]:= VykresliGraf[Scaling]
```

Zdrojový kód 37 Změna měřítka objektu



Obr. 3 Graf změny měřítka objektu

4. Transformace otočení

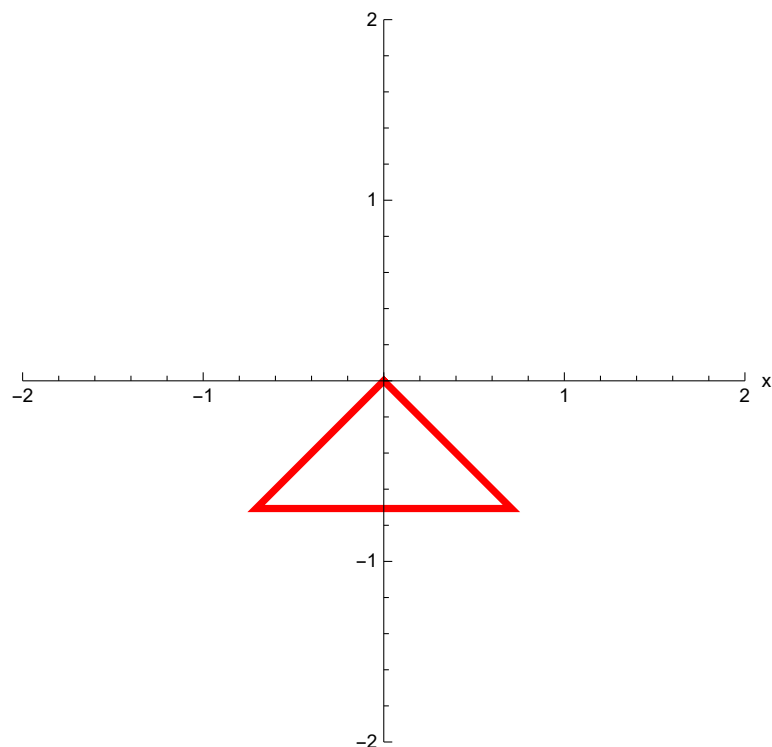
```

1 In[571]:= uhel = 135;
2 In[572]:= RotateM={{Cos[uhel Degree],Sin[uhel Degree
    ],0},{-Sin[uhel Degree],Cos[uhel Degree],0},{0,0,1}};
3 In[573]:= Rotation = RotateM.Basic;
4 MatrixForm[RotateM].MatrixForm[Basic] ->
5 MatrixForm[Rotation]
6
7 Out[34]= 
$$\begin{pmatrix} 1 & 1 & 0 \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 0 \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

8
9
10
11 In[575]:= BodyObjektu[Rotation]
12 Out[575]= {{0, 0}, {-1/2, -1/2}, {1/2, -1/2}}
13
14 In[576]:= VykresliGraf[Rotation]

```

Zdrojový kód 38 Otočení objektu

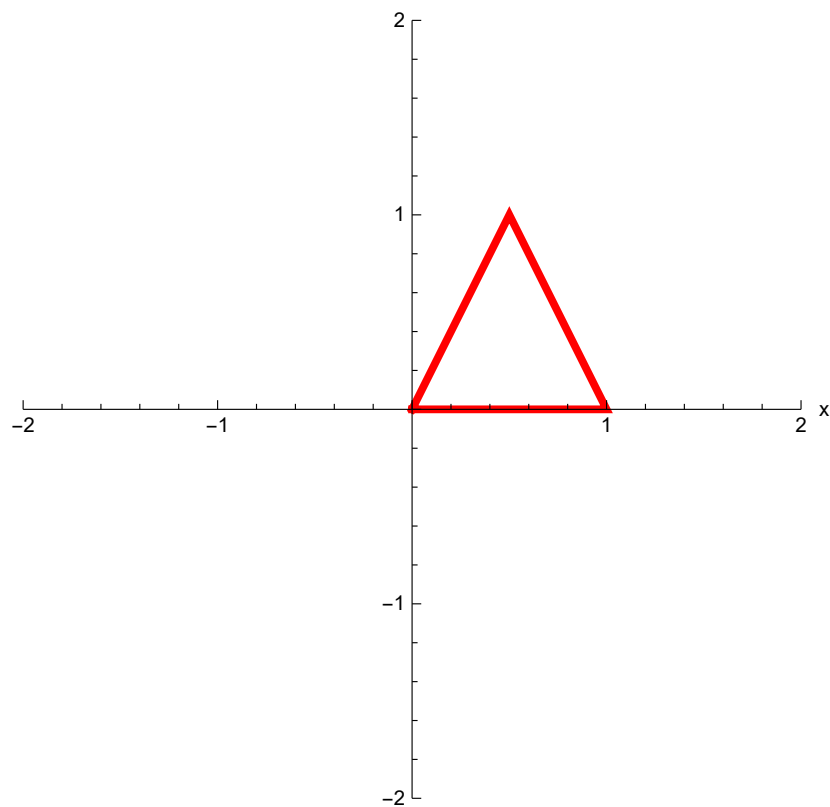


Obr. 4 Graf otočení objektu

5. Zkosení podle osy x

```
1 In[624]:= shxM={{1,0.5,0},{0,1,0},{0,0,1}};  
2 ShearX = shxM.Basic;  
3 MatrixForm[shxM].MatrixForm[Basic] ->  
4 MatrixForm[ShearX]  
5  
6 Out[34]=  $\begin{pmatrix} 1 & 0.5 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0.5 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$   
7  
8  
9  
10 In[627]:= BodyObjektu[ShearX]  
11 Out[627]= {{0., 0.}, {1., 0.}, {0.5, 1.}}  
12  
13 In[628]:= VykresliGraf[ShearX]
```

Zdrojový kód 39 Zkosení objektu podle osy x

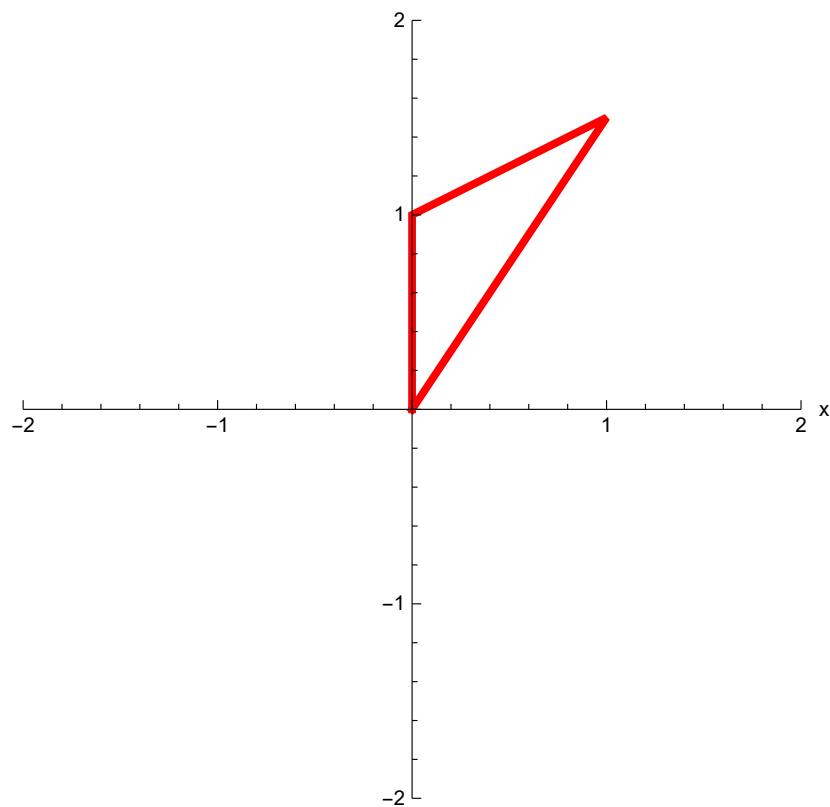


Obr. 5 Graf zkosení objektu dle osy x

6. Zkosení podle osy y

```
1 In[624]:= shyM={{1,0,0},{1.5,1,0},{0,0,1}};  
2 ShearY = shyM.Basic;  
3 MatrixForm[shyM].MatrixForm[Basic] ->  
4 MatrixForm[ShearY]  
5  
6 Out[34]= 
$$\begin{pmatrix} 1 & 0 & 0 \\ 1.5 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 1.5 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$
  
7  
8  
9  
10 In[627]:= BodyObjektu[ShearY]  
11 Out[627]= {{0., 0.}, {1., 1.5}, {0., 1.}}  
12  
13 In[628]:= VykresliGraf[ShearY]
```

Zdrojový kód 40 Zkosení objektu podle osy y

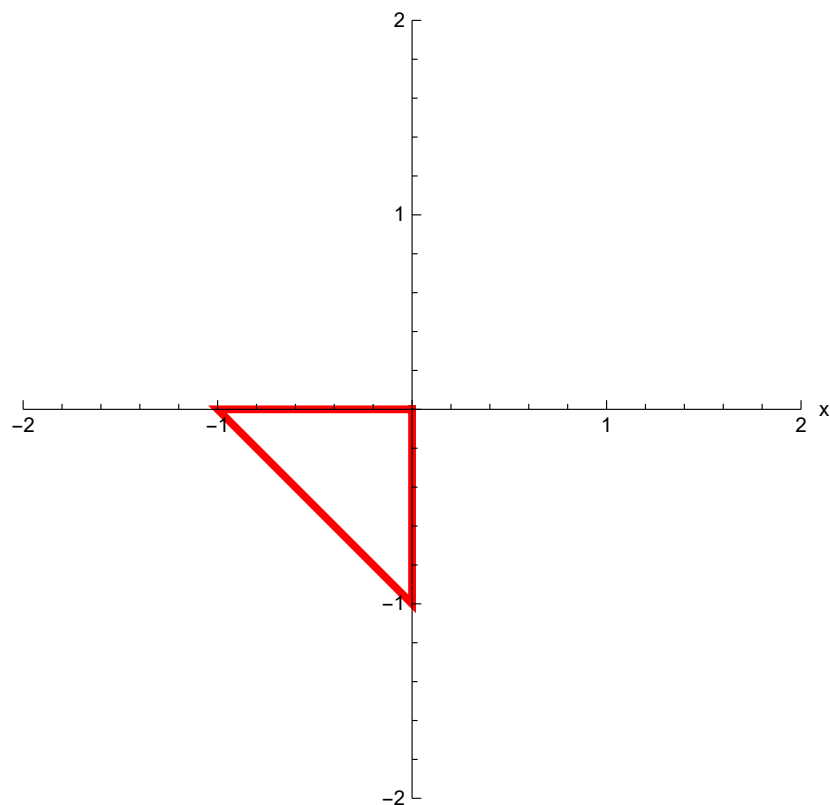


Obr. 6 Graf zkosení objektu dle osy y

7. Zrcadlení podle počátku soustavy souřadnic

```
1 In[634]:= ReflectM = {{-1, 0, 0}, {0, -1, 0}, {0, 0, 1}};  
2 Reflection = ReflectM.Basic;  
3 MatrixForm[ReflectM].MatrixForm[Basic] ->  
4 MatrixForm[Reflection]  
5  
6 Out[34]=
$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$
  
7  
8  
9  
10 In[637]:= BodyObjektu[Reflection]  
11 Out[637]= {{0, 0}, {-1, 0}, {0, -1}}  
12  
13 In[638]:= VykresliGraf[Reflection]
```

Zdrojový kód 41 Zrcadlení podle počátku soustavy souřadnic

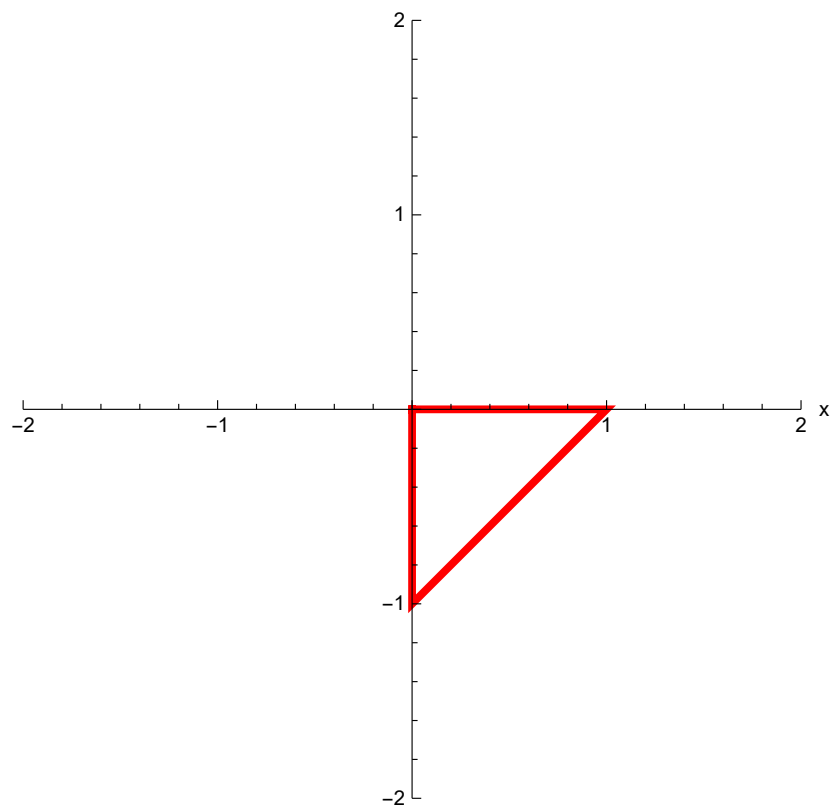


Obr. 7 Graf zrcadlení podle počátku soustavy souřadnic

8. Zrcadlení podle osy x

```
1 In[634]:= ReflectXM = {{1, 0, 0}, {0, -1, 0}, {0, 0, 1}};  
2 ReflectionX = ReflectXM.Basic;  
3 MatrixForm[ReflectXM].MatrixForm[Basic] ->  
4 MatrixForm[ReflectionX]  
5  
6 Out[34]= 
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$
  
7  
8  
9  
10 In[637]:= BodyObjektu[ReflectionX]  
11 Out[637]= {{0, 0}, {1, 0}, {0, -1}}  
12  
13 In[638]:= VykresliGraf[ReflectionX]
```

Zdrojový kód 42 Zrcadlení podle osy x

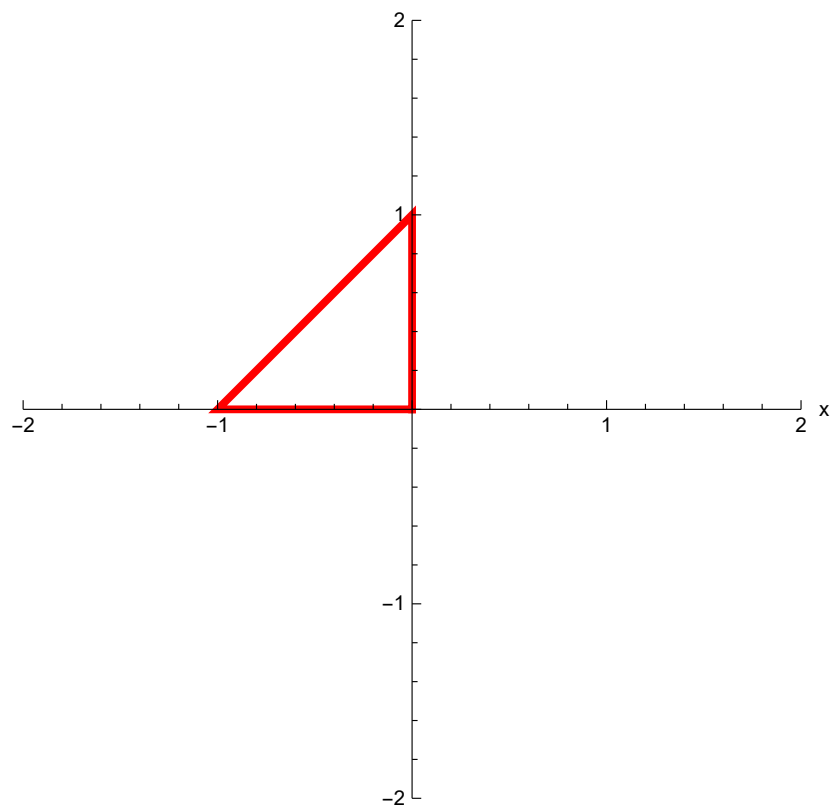


Obr. 8 Graf zrcadlení objektu podle osy x

9. Zrcadlení podle osy y

```
1 In[634]:= ReflectYM = {{-1, 0, 0}, {0, 1, 0}, {0, 0, 1}};  
2 ReflectionY = ReflectYM.Basic;  
3 MatrixForm[ReflectYM].MatrixForm[Basic] ->  
4 MatrixForm[ReflectionY]  
5  
6 Out[34]= 
$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$
  
7  
8  
9  
10 In[637]:= BodyObjektu[ReflectionY]  
11 Out[637]= {{0, 0}, {-1, 0}, {0, 1}}  
12  
13 In[638]:= VykresliGraf[ReflectionY]
```

Zdrojový kód 43 Zrcadlení podle osy Y



Obr. 9 Graf zrcadlení objektu podle osy y

10. Skládání transformací

Na základní matici jsou postupně aplikované transformace změny měřítka, rotace, zkosení podle osy x a zrcadlení podle počátku. V tomto pořadí.

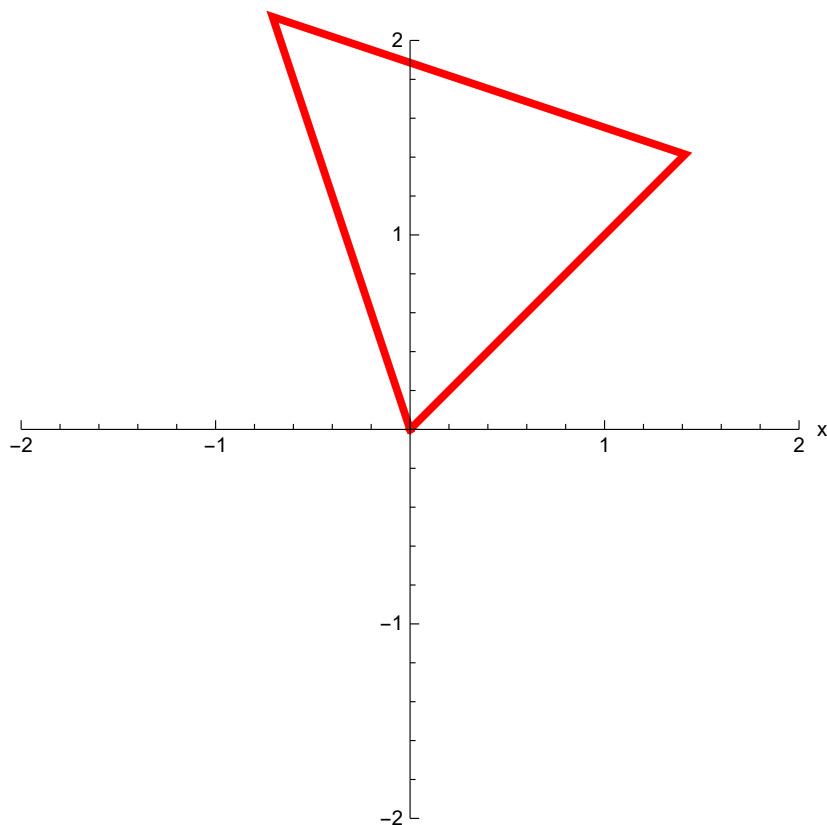
```

1 In[456]:= CompM = ScaleMatrix.RotateMatrix.shx.reflect;
2 In[457]:= Comp = CompM.Basic;
3 MatrixForm[CompM].MatrixForm[Basic] -> MatrixForm[Comp]
4
5      
$$\text{Out}[34] = \begin{pmatrix} 1.41 & -0.70 & 0 \\ 1.41 & 2.12 & 0 \\ -1 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1.41 & -0.70 & 0 \\ 1.41 & 2.12 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

6
7
8
9 In[637]:= BodyObjektu[Comp]
10 Out[637]= {{0., 0.}, {1.41, 1.41}, {-0.70, 2.12}}
11 In[638]:= VykresliGraf[Comp]

```

Zdrojový kód 44 Skládání transformací



Obr. 10 Graf skládání transformací

ZÁVĚR

Cílem této práce bylo seznámit čtenáře se základním oborem matematiky, kterým je lineární algebra. Text bakalářské práce byl vytvořen jako podpůrný text pro studenty navštěvující Math Support Centre. Témata, která jsou probírána se řadí mezi ty nejzákladnější a nejnutnější k pochopení principu fungování lineární algebry.

V první polovině bakalářské práce jsem vysvětlil pojem vektorový prostor, co musí vektorové prostory splňovat a jejich vybrané příklady. Za těmito příklady je uvedena také teorie lineárních kombinací vektorů. Následuje teorie týkající se matic. Ta obsahuje podkapitoly jako je představení různých typů matic, operace s maticemi a elementární úpravy matic.

V druhé polovině práce se zabývám determinanty a teorií s nimi spjatou. Ilustruji výpočty determinantů pro různé velké čtvercové matice, za kterými následuje definice inverzních matic. V následující kapitole je probrána teorie lineárních rovnic a hlavně způsoby, jakými soustavy počítat.

Veškeré příklady uvedené v práci jsou řešeny tak, aby jim porozuměl i naprostý laik. K dispozici jsou slovně popsány postupy a možnosti řešení. Pro ještě lepší představu jsou představeny možnosti řešení v matematickém software Wolfram Mathematica. Tento program je velice vhodné pro účely výuky lineární algebry, jelikož je snadno ovladatelný a srozumitelný.

Lineární algebra je jeden ze stavebních kamenů matematiky a studenti by se s ní neměli setkávat až na vysokých školách. Matematika jako taková se jeví mnohem snazší s poznatky, které vzniknou studiem této disciplíny. Srdečně doufám, že tyto podpůrné materiály najdou uplatnění v již zmíněném centru a pomohou studentům Univerzity Tomáše Bati nejenom z fakulty aplikované informatiky.

SEZNAM POUŽITÉ LITERATURY

- [1] HORT, Daniel a Jiří RACHŮNEK. *Algebra I*. Olomouc: Univerzita Palackého v Olomouci, 2003. ISBN 80-244-0631-4.
- [2] BICAN, Ladislav. *Lineární algebra a geometrie*. Praha: Akademie věd České republiky, 2002. ISBN 80-200-0843-8.
- [3] KRUPKOVÁ, Olga. *Lineární algebra 1* [online]. Olomouc: Univerzita Palackého Olomouc, 2008 [cit. 2018-03-07]. Dostupné z: <http://phoenix.inf.upol.cz/esf/ucebni/Algebra.pdf>
- [4] OLŠÁK, Petr. *Lineární algebra* [online]. Praha: Univerzita Karlova, 2008 [cit. 2018-03-07]. Dostupné z: <http://petr.olsak.net/ftp/olsak/linal/linal.pdf>
- [5] Determinanty, matice a Sarrusovo pravidlo. In: *Aristoteles* [online]. [cit. 2018-03-07]. Dostupné z: <http://www.aristoteles.cz/matematika/linearni-algebra/determinanty/determinanty-a-matice-sarrusovo-pravidlo.php>
- [6] JUKL, Marek. *Lekce z lineární algebry* [online]. Olomouc, 2012 [cit. 2018-03-07]. Dostupné z: <http://www.kag.upol.cz/data/upload/15/Lekce-z-linearni-algebry.pdf>
- [7] EMANOVSKÝ, Petr a Jan KÜHR. *Cvičení z algebry pro 1. ročník I*. Olomouc: Univerzita Palackého, 2007. ISBN 978-80-244-1833-9.
- [8] BARTO, Libor a Jiří TŮMA. *Lineární algebra* [online]. Praha: Univerzita Karlova, 2015 [cit. 2018-03-07]. ISBN 978-80-244-1833-9. Dostupné z: <http://www.karlin.mff.cuni.cz/~sir/la/LinAlg/skripta.pdf>
- [9] BICAN, Ladislav. *Lineární algebra: Určeno por posl. vys. škol*. 1. vyd. Praha: SNTL, 1979. 331, [1] s. Řada teoretické lit. Matematický seminář SNTL, sv. 14.
- [10] KRUPKOVÁ, Vlasta a Petr FUCHS. *Matematika I* [online]. Brno: Vysoké učení technické v Brně, 2014 [cit. 2018-03-07]. Dostupné z: <http://www.umat.feec.vutbr.cz/~krupkova/linalgx.pdf>
- [11] JIŘÍ, Žára a Jiří ŽÁRA. *Moderní počítačová grafika*. Brno: Computer Press, 2004. ISBN 80-251-0454-0.

-
- [12] CAYLEY, A. *A Memoir on the Theory of Matrices*. Philosophical Transactions of the Royal Society of London (1776-1886). 1858-01-01. 148:17–37
- [13] TOLKIEN, John Ronald Reuel. *The Fellowship of the Ring*. Velká Británie: George Allen and Unwin, 1954. ISBN 0-345-33970-3.

SEZNAM OBRÁZKŮ

Obr. 1	Graf základního objektu	56
Obr. 2	Graf posunutí objektu	57
Obr. 3	Graf změny měřítka objektu	58
Obr. 4	Graf otočení objektu	59
Obr. 5	Graf zkosení objektu dle osy x	60
Obr. 6	Graf zkosení objektu dle osy y	61
Obr. 7	Graf zrcadlení podle počátku soustavy souřadnic	62
Obr. 8	Graf zrcadlení objektu podle osy x	63
Obr. 9	Graf zrcadlení objektu podle osy y	64
Obr. 10	Graf skládání transformací	65

SEZNAM ZDROJOVÝCH KÓDŮ

1	Definice vektorů $\vec{u}, \vec{v}, \vec{w}$ a skalárů a, b	12
2	Ověření platnosti axiomů	12
3	Výpočet lineární kombinace vektorů	14
4	Ověření lineární závislosti	15
5	Vytvoření matice A	17
6	Vypsání prvku a_{12} a prvku a_{22}	17
7	Výpis druhého a třetího řádku	17
8	Výpis prvního a třetího sloupce	17
9	Součet dvou matic	20
10	Rozdíl dvou matic	21
11	Násobení matice skalárem	22
12	Násobení matic	24
13	Přičtení druhého sloupce matice k sloupci třetímu	26
14	Vynásobení prvního sloupce matice číslem 2	26
15	Výměna sloupců matice	26
16	Permutace	29
17	Výpočet determinantu	35
18	Inverzní matice	38
19	Řešení soustavy rovnic	42
20	Gaussova eliminační metoda	43
21	Cramerovo pravidlo	46
22	Vytvoření abecedy a zprávy	48
23	Matice klíče	48
24	Inverzní klíč	49
25	Vytvoření asociace znaků s čísly	49
26	Funkce doplnění zprávy	50
27	Funkce aplikace šifrovacího klíče	50
28	Funkce převodu čísel na text	50
29	Funkce Hillova šifrování	51
30	Zvolení abecedy a vložení textu	51
31	Šifrování textu	51
32	Dešifrování textu	52
33	Funkce pro vytvoření bodů objektu	55
34	Funkce pro vykreslení grafu objektu	55
35	Vytvoření základního objektu	56
36	Posunutí objektu	57

37	Změna měřítka objektu	58
38	Otočení objektu	59
39	Zkosení objektu podle osy x	60
40	Zkosení objektu podle osy y	61
41	Zrcadlení podle počátku soustavy souřadnic	62
42	Zrcadlení podle osy x	63
43	Zrcadlení podle osy Y	64
44	Skládání transformací	65

SEZNAM PŘÍLOH

P I. Obsah přiloženého CD

PŘÍLOHA P I. OBSAH PŘILOŽENÉHO CD

Příloha CD obsahuje následující soubory:

1. Zdrojové kódy programu Wolfram Mathematica použité v bakalářské práci
2. Dokumentace programu Wolfram Mathematica
3. Bakalářská práce ve formátu PDF