# ALGEBRA I

**Daniel Hort, Jiří Rachůnek**

Univerzita Palackého
OLOMOUC 2003

# Předmluva

Hlavním obsahem učebního textu je úvod do lineární algebry, tedy předmětu, který je využíván v mnoha dalších matematických a i nematematických disciplínách. Text je určen pro posluchače prvního, a částečně i druhého, semestru, kteří na Přírodovědecké fakultě UP studují ve studijních programech 1101R Matematika a 1801R Informatika studijní obory Diskrétní matematika, Matematika a její aplikace, Matematika dvouoborová (učitelská) a Informatika.

Ve snaze, aby k četbě a studiu podle skripta postačovaly znalosti matematiky ze střední školy na úrovni gymnázia, byly do něj zařazeny i první dvě kapitoly obsahující základní poznatky z matematické logiky a teorie množin v nezbytném rozsahu. Do třetí kapitoly jsou zařazeny aspoň orientačně základní algebraické struktury s binárními operacemi, přestože jejich důkladnější studium je obsahem až dalších semestrů. Pojmy a jednoduché výsledky z této kapitoly umožňují jednodušší vyjadřování i orientaci v látce dalších kapitol, které jsou už věnovány lineární algebře. Při studiu lineární algebry se však také získávají obecné struktury, jejichž prvky nemusí být čísla a které budou i později sloužit jako vhodné modely při teoretickém výkladu binárních algebraických struktur.

Teoretická látka, která je v učebním textu probírána, je ilustrována na příkladech. Čtenář si může také ověřit také pochopení a zvládnutí látky při řešení cvičení uvedených za jednotlivými kapitolami.

V textu je použito standardního označení pro nejpoužívanější číselné množiny, jak je uvedeno v následujícím přehledu:

$\mathbb{N}$ ........ množina všech přirozených čísel
$\mathbb{Z}$ ........ množina všech celých čísel
$\mathbb{Q}$ ........ množina všech racionálních čísel
$\mathbb{R}$ ........ množina všech reálných čísel
$\mathbb{C}$ ........ množina všech komplexních čísel
$\mathbb{Z}_0, \mathbb{Q}_0, \mathbb{R}_0, \mathbb{C}_0$ množina všech nenulových celých (racionálních, reálných, komplexních) čísel
$\mathbb{Q}^+, (\mathbb{R}^+)$ ........ množina všech kladných racionálních (reálných) čísel
$\mathbb{Z}^+, (\mathbb{Q}_0^+, \mathbb{R}_0^+)$ ........ množina všech nezáporných celých (racionálních, reálných) čísel
$\mathbb{Z}^-, (\mathbb{Q}^-, \mathbb{R}^-)$ ........ množina všech záporných celých (racionálních, reálných) čísel

Pro větší přehlednost je konec důkazu každé věty označen symbolem „$\square$“

Prosinec 2002 Autoři

# Kapitola 1

# Základy matematické logiky

## 1.1 Formalizace jazyka

Dobře víme, že pro studium matematiky i pro možnost jejího použití je zapotřebí velice přesného vyjadřování. Ukažme si, že živý jazyk je často málo přesný a přitom zbytečně komplikovaný.

**Příklad 1.1** Všimněme si věty
„Číslo $n$ je nejmenší přirozené číslo, které není možno charakterizovat pomocí věty českého jazyka s nejvýše šedesáti slabikami."
Přitom ale tato věta, která má méně než 60 slabik, charakterizuje číslo $n$, proto $n$ nemůže mít popisovanou vlastnost. Tento paradox je důsledkem nepřesného používání živého jazyka.

**Příklad 1.2** Je zřejmé, že zápis rovnosti

$$(a+b)^2 = a^2 + 2ab + b^2,$$

kde $a, b$ jsou libovolná komplexní čísla, není větou českého jazyka. Pokud bychom chtěli tuto rovnost vyjádřit slovně, museli bychom použít velmi komplikovaného tvrzení následujícího typu:
„Druhá mocnina součtu libovolných dvou komplexních čísel se rovná součtu tří členů, z nichž první je druhou mocninou prvního čísla, druhý je dvojnásobkem součinu obou čísel a třetí je druhou mocninou druhého čísla.".

Vidíme tedy, že je účelné vybudovat pro matematické teorie přesný specializovaný a *formalizovaný* jazyk. K tomu je především nutné určit *symboly*, kterých se bude používat. Souboru všech těchto symbolů budeme říkat *abeceda*. Konečné posloupnosti symbolů z abecedy nazveme *slova vytvořená v dané abecedě* nebo také *slova nad danou abecedu*.

**Příklad 1.3** Předpokládejme, že do dané abecedy patří symboly $x, y, +, (, ), =, 1, 2, 3$. Potom výrazy

$$(x+y), x+y = y+x, x++ = (33,\ 12111$$

jsou slova nad touto abecedou.

Z příkladu je vidět, že ne všechna slova nad abecedou dané teorie budou pro studovanou teorii užitečná. Proto budeme muset vyčlenit ze systému všech slov systém „vhodných“ slov, kterým také můžeme říkat *správně utvořená slova*.

**Příklad 1.4** V příkladu 1.3 budeme zřejmě za „vhodná“ slova považovat taková slova, která dávají smysl v aritmetice přirozených čísel. Jsou to např. slova

$$x + y = y + x, 12 + 3 = 11, 11 + 2 = 13.$$

Pro přesné studium dané teorie musíme také určit pravidla, kterých budeme při úvahách používat. Základem úvah ve všech matematických teoriích je matematická logika. V matematických teoriích dále rozdělíme symboly z používané abecedy do dvou skupin, na tzv. konstanty a proměnné.

**Definice 1.1**

*a)* Konstantou *rozumíme každý jazykový výraz, který má jednoznačně určený smysl.*

*b)* Proměnnou *rozumíme každý jazykový výraz, který sám nemá smysl, ale který určuje místo, na které je možné za něj dosazovat konstanty z daného oboru proměnnosti.*

**Příklad 1.5** V příkladu 1.3 jsou konstantami symboly $1, 2, 3, +, (, ), =$ a proměnnými jsou $x, y$.

## 1.2 Výroková logika

V této části si připomeneme a upřesníme základní pojmy a vztahy týkající se výrokové logiky.

**Definice 1.2** Výrok *je každé sdělení, o kterém má smysl uvažovat, zda je nebo není pravdivé, přičemž může nastat právě jedna z těchto dvou možností.*

Uvědomme si, že podle této definice považujeme za výroky i taková sdělení, u nichž neumíme v daném okamžiku rozhodnout o jejich pravdivosti, tedy za výroky považujeme i všechny hypotézy. Takže např. věta

„Ve vesmíru existuje život i mimo Zemi.“

je výrokem.

Jak je zvykem, budeme pravdivým výrokům přiřazovat číslo 1, nepravdivým výrokům číslo 0. Číslům 0 a 1 říkáme *pravdivostní hodnoty* výroků. Z výroků můžeme vytvářet složitější výroky pomocí *výrokových spojek*. Budeme všude používat jen tzv. *extenzionálních spojek*, tj. takových spojek, pro které je pravdivostní hodnota vzniklého výroku závislá pouze na pravdivostních hodnotách spojovaných výroků a na používané spojce.

Než přistoupíme k popisu spojek, vyslovíme následující definici.

**Definice 1.3**

a) *Výrok, ve kterém neexistuje žádná jeho vlastní část, která by byla výrokem, se nazývá* atomární výrok.

b) *Každý jiný výrok se nazývá* složený výrok.

**Příklad 1.6** Výrok „Šest je dělitelné třemi a šest je dělitelné dvěma.“ je složený, zatímco výroky „Šest je dělitelné třemi.“ a „Šest je dělitelné dvěma.“ jsou atomární.

Nyní si připomeňme výrokové spojky, které se běžně používají na střední škole a které budou postačovat i pro naše účely. Podle počtu spojovaných výroků rozdělíme spojky na *unární*, neboli *jednoargumentové*, a *binární*, neboli *dvouargumentové*.

Extenzionální unární spojky jsou celkově čtyři, nám však bude postačovat jediná - *negace*. Je-li $A$ výrok, pak jeho negaci označíme $\neg A$ a pravdivostní hodnotu negace v závislosti na daném výroku určíme takto:

| A | $\neg A$ |
|---|---|
| 1 | 0 |
| 0 | 1 |

Podle této tabulky je negace $A$ pravdivého výroku $A$ nepravdivým výrokem a naopak. Binárních extenzionálních spojek je celkově 16.

| A | B | $T$ | $\vee$ | $\Leftarrow$ | A | $\Rightarrow$ | B | $\Leftrightarrow$ | $\wedge$ | $\mid$ | $\veebar$ | $\neg B$ | $\not\Rightarrow$ | $\neg A$ | $\not\Leftarrow$ | $\downarrow$ | $K$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |

$\downarrow$-Nicodova spojka, $\mid$-Shefferova spojka, $T$-tautologie, $K$-kontradikce

Podrobněji si popíšeme 4 nejpoužívanější.
*Konjunkci* výroků $A$ a $B$ označíme $A \wedge B$ a její pravdivostní hodnota je dána takto:

| A | B | $A \wedge B$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 0 |

Konjunkci čteme „$A$ a $B$“, popř. „$A$ a současně $B$“, a vidíme, že je pravdivá právě v případě, kdy každý z výroků $A$ a $B$ je pravdivý.

*Disjunkci* výroků $A$ a $B$ označíme $A \vee B$ a její pravdivostní hodnota je v závislosti na pravdivostních hodnotách výroků $A$ a $B$ určena tabulkou:

| A | B | $A \vee B$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 0 |

Disjunkce $A \vee B$ je tedy pravdivá, je-li alespoň jeden z výroků $A, B$ pravdivý, a čteme ji „$A$ nebo $B$“. Spojka „nebo“ je tak chápána v nevylučovacím slova smyslu.

*Implikace* výroků $A$ a $B$ je označena $A \Rightarrow B$ a je dána tabulkou:

| A | B | $A \Rightarrow B$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 1 |
| 0 | 0 | 1 |

podle níž je implikace nepravdivá právě tehdy, když výrok $A$ je pravdivý a výrok $B$ nepravdivý. Implikaci $A \Rightarrow B$ čteme „Jestliže $A$, pak $B$.“, „Platí-li $A$, pak $B$.“, „$A$ implikuje $B$.“, „$A$ je postačující podmínka pro $B$.“, „$B$ je nutná podmínka pro $A$.“, apod.

*Ekvivalenci* výroků $A$ a $B$ označíme $A \Leftrightarrow B$ a je dána tabulkou:

| A | B | $A \Leftrightarrow B$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 1 |

Vidíme, že ekvivalence $A \Leftrightarrow B$ je pravdivá, nabývají-li výroky $A$ a $B$ stejných pravdivostních hodnot, a je nepravdivá v opačném případě. Čteme ji „$A$ tehdy a jen tehdy, když $B$.“, „$A$ právě tehdy, když $B$.“, „ $A$ je nutná a postačující podmínka pro $B$.“, „$A$ je ekvivalentní s $B$.“.

V dalším se budeme věnovat otázkám, jak závisí pravdivostní hodnota složeného výroku na pravdivostních hodnotách skládaných výroků. Teorie, která se těmito problémy zabývá, se nazývá *výrokový počet*. Pro výrokový počet, jako pro každou formalizovanou teorii, musíme nejdříve určit abecedu, kterou budeme používat. Zařadíme do ní tyto symboly

$$\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow, (, ),$$

které budou konstantami a symboly

$$A, B, C, \dots,$$

které budou proměnnými (tzv. *výrokovými proměnnými*). Podle potřeby můžeme za obor proměnnosti libovolné výrokové proměnné považovat buď dvouprvkovou množinu $\{0, 1\}$ nebo množinu všech výroků. (Uvědomme si, že výrokových proměnných jsme už vlastně používali při popisu jednotlivých výrokových spojek.)

Správně vytvořená slova výrokové logiky nazveme *formulemi výrokové logiky* a definujeme je takto:

**Definice 1.4**

*a) Každá výroková proměnná je formulí výrokové logiky.*

*b) Jsou-li slova $\mathcal{A}$ a $\mathcal{B}$ formulemi výrokové logiky, pak jsou také slova*

$$\neg(\mathcal{A}), (\mathcal{A}) \wedge (\mathcal{B}), (\mathcal{A}) \vee (\mathcal{B}), (\mathcal{A}) \Rightarrow (\mathcal{B}), (\mathcal{A}) \Leftrightarrow (\mathcal{B})$$

*formulemi výrokové logiky.*

*c) Slovo je formulí výrokové logiky právě tehdy, je-li možné je získat pomocí a) a b) v konečném počtu kroků.*

Volně řečeno, platí tedy, že slovo je formulí výrokové logiky, vznikne-li z výrokových proměnných postupným „správným“ používáním výrokových spojek.

Všimněme si toho, že symboly $\mathcal{A}$ a $\mathcal{B}$ z definice nejsou symboly výrokového počtu. Jsou to vlastně proměnné, za které můžeme dosazovat formule výrokové logiky. Takovýmto symbolům se říká také *metasymboly* dané teorie.

Dohodněme se, že při zápisu formulí výrokové logiky budeme vynechávat zbytečné závorky, a že budeme používat také jiných typů závorek.

**Příklad 1.7** Slovo

$$((\neg(A)) \vee ((B) \Rightarrow (C))) \Leftrightarrow ((C) \Rightarrow ((\neg(B)) \wedge (A)))$$

je podle definice 1.4 formulí výrokové logiky a budeme je zapisovat zjednodušeně ve tvaru

$$[\neg(A \vee (B \Rightarrow C))] \Leftrightarrow [C \Rightarrow (\neg B \wedge A)].$$

Slovo $((A) \Rightarrow ((B)\neg \vee (C)))$ samozřejmě není formulí výrokové logiky.

U konkrétních formulí výrokové logiky nás bude zajímat, jakých pravdivostních hodnot nabývají tyto formule v závislosti na pravdivostních hodnotách výrokových proměnných, které jsou v těchto formulích obsaženy. Je zřejmé, že obsahuje-li formule výrokové logiky $n$ proměnných, pak existuje $2^n$ možností, jak dosazovat za tyto proměnné pravdivostní hodnoty 0 a 1. Pro zjišťování pravdivostních hodnot formulí výrokové logiky používáme s výhodou tzv. *tabulkové metody*. Tato spočívá v sestavení tabulky, která má $2^n$ řádků a $n+1$ sloupců, kde v jednotlivých řádcích zapíšeme na prvních $n$ místech postupně všechny možnosti dosazení hodnot 0 a 1 za výrokové proměnné a v $(n+1)$-ním sloupci je odpovídající pravdivostní hodnota dané formule. Přitom pravdivostní hodnotu formule určíme dosazením zvolených pravdivostních hodnot za jednotlivé proměnné a postupným používáním definic výrokových spojek.

**Příklad 1.8** Určete pravdivostní hodnotu formule

$$(A \vee \neg B) \Rightarrow [B \Leftrightarrow (A \wedge \neg C)].$$

Tato formule obsahuje 3 výrokové proměnné, proto k určení pravdivostních hodnot bude užito tabulky, která bude mít 8 řádků a 4 sloupce. (Pravdivostní hodnoty dané formule jsou zapsány pod spojkou $\Rightarrow$.)

| A | B | C | (A | ∨ | ¬ | B) | ⇒ | [B | ⇔ | (A | ∧ | ¬ | C ] |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 |

`Poznámka:` Při určování pravdivostních hodnot formulí pomocí tabulkové metody není nutné vždy určovat pro každý řádek všechny postupné výsledky. S výhodou používáme specifických vlastností některých spojek. Např. je-li jeden člen konjunkce nepravdivý, je celá konjunkce nepravdivá, je-li jeden člen disjunkce pravdivý, je celá disjunkce pravdivá, apod.

**Příklad 1.9** Určete pravdivostní hodnotu formule

$$[(A \Rightarrow B) \wedge (B \Rightarrow C)] \Rightarrow (A \Rightarrow C).$$

Budeme se snažit zkrátit řešení podle předchozí poznámky.

| A | B | C | [(A | ⇒ | B) | ∧ | (B | ⇒ | C)] | ⇒ | (A | ⇒ | C) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | | | | | | | | 1 | | 1 | 1 |
| 1 | 1 | 0 | | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| 1 | 0 | 1 | | | | | | | | 1 | | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | | 1 | 1 | 0 | 0 |
| 0 | 1 | 1 | | | | | | | | 1 | 0 | 1 | |
| 0 | 1 | 0 | | | | | | | | 1 | 0 | 1 | |
| 0 | 0 | 1 | | | | | | | | 1 | 0 | 1 | |
| 0 | 0 | 0 | | | | | | | | 1 | 0 | 1 | |

Zde jsme využívali zejména skutečnosti, že je-li levý člen implikace pravdivý, pak je celá implikace pravdivá. Přitom jsme nejdříve vyhodnocovali pravou stranu implikace, protože je jednodušší než levá strana.

Všimněme si ještě jednou pravdivostních hodnot formulí v příkladech 1.8 a 1.9. Zatímco formule z příkladu 1.8 nabývá pro některá dosazení za proměnné hodnotu 1 a pro některá hodnotu 0, formule z příkladu 1.9 nabývá ve všech řádcích hodnotu 1. Formule mající stejnou vlastnost jako poslední formule jsou pro matematiku (a pro správné myšlení vůbec) nejdůležitější.

**Definice 1.5** *Formuli výrokové logiky, jejíž pravdivostní hodnota je rovna 1 pro každé dosazení pravdivostních hodnot za výrokové proměnné, nazýváme* tautologie.

Opakem tautologie je *kontradikce*.

Tautologie jsou vlastně logickými zákony, protože dosadíme-li do nich za proměnné libovolné výroky, bude výsledný složený výrok vždy pravdivý. Uveďme si proto několik nejčastěji používaných tautologií.

| | | |
|---|---|---|
| 1. | $A \vee \neg A$ | (zákon vyloučeného třetího) |
| 2. | $\neg(A \wedge \neg A)$ | (zákon sporu) |
| 3. | $\neg(\neg A) \Leftrightarrow A$ | (zákon dvojí negace) |
| 4. | $(A \wedge B) \Leftrightarrow (B \wedge A)$ | (zákon komutativní pro konjunkci) |
| 5. | $(A \vee B) \Leftrightarrow (B \vee A)$ | (zákon komutativní pro disjunkci) |
| 6. | $[A \wedge (B \wedge C)] \Leftrightarrow [(A \wedge B) \wedge C]$ | (zákon asociativní pro konjunkci) |
| 7. | $[A \vee (B \vee C)] \Leftrightarrow [(A \vee B) \vee C]$ | (zákon asociativní pro disjunkci) |
| 8. | $[A \wedge (B \vee C)] \Leftrightarrow (A \wedge B) \vee (A \wedge C)$ | (zákon distributivní - konjunkce je distributivní vzhledem k disjunkci) |
| 9. | $[A \vee (B \wedge C)] \Leftrightarrow (A \vee B) \wedge (A \vee C)$ | (zákon distributivní - disjunkce je distributivní vzhledem ke konjunkci) |
| 10. | $(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$ | |
| 11. | $\neg(A \Rightarrow B) \Leftrightarrow (A \wedge \neg B)$ | |
| 12. | $\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B)$ | (de Morganův zákon) |
| 13. | $\neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B)$ | (de Morganův zákon) |
| 14. | $(A \Leftrightarrow B) \Leftrightarrow [(A \Rightarrow B) \wedge (B \Rightarrow A)]$ | |
| 15. | $[(A \Rightarrow B) \wedge (B \Rightarrow C)] \Longrightarrow (A \Rightarrow C)$ | (tranzitivita implikace) |
| 16. | $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$ | (zákon kontrapozice) |
| 17. | $A \Leftrightarrow A \wedge (B \vee \neg B)$ | |
| 18. | $A \Rightarrow (B \Rightarrow C) \Leftrightarrow (A \wedge B) \Rightarrow C$ | |
| 19. | $(A \Leftrightarrow B) \Leftrightarrow (\neg A \Leftrightarrow \neg B)$ | |
| 20. | $(A \Leftrightarrow B) \Leftrightarrow (\neg A \vee B) \wedge (A \vee \neg B)$ | |
| 21. | $A \Leftrightarrow A \wedge (A \vee B)$ | |
| 22. | $A \Leftrightarrow A \vee (A \wedge B)$ | |

Využijeme ještě pojmu tautologie k zavedení následujících pojmů.

**Definice 1.6**

a) *Jsou-li $\mathcal{A}$ a $\mathcal{B}$ formule výrokové logiky a je-li implikace $\mathcal{A} \Rightarrow \mathcal{B}$ tautologií, pak řekneme, že z $\mathcal{A}$* logicky vyplývá *$\mathcal{B}$.*

b) *Je-li $\mathcal{A} \Leftrightarrow \mathcal{B}$ tautologie, pak říkáme, že formule $\mathcal{A}$ a $\mathcal{B}$ jsou* logicky ekvivalentní.

## 1.3 Predikátová logika

Ve výrokové logice jsou atomární výroky uvažovány jako celek a zajímáme se pouze o jejich pravdivost nebo nepravdivost. V matematice ale bude pro nás důležitá i vnitřní stavba některých typů výroků. K tomuto slouží predikátová logika, jejíž základy si nyní připomeneme.

**Definice 1.7** Výroková forma *je každé takové sdělení, které obsahuje proměnné a které se stane výrokem po dosazení konstant z oborů proměnnosti za všechny proměnné.*

**Příklad 1.10** Následující sdělení jsou výrokovými formami:

a) $x$ je dělitelné pěti. ($x$ ... přirozené číslo)

b) $x$ je dělitelné $y$. ($x, y$ ... přirozená čísla)

c) Bod $a$ leží na přímce $p$. ($a$ ... bod v rovině, $p$ ... přímka v téže rovině)

Přitom první z těchto výrokových forem obsahuje jednu proměnou a dostaneme z ní výrok po dosazení libovolného přirozeného čísla za tuto proměnnou, zbývající dvě výrokové formy obsahují dvě proměnné a výrokové formy přejdou ve výroky po dosazení konstant z příslušných oborů proměnnosti za obě proměnné.

Výrokové formy můžeme spojovat (podobně jako výroky) pomocí výrokových spojek. Výsledkem jsou opět výrokové formy.

Definice 1.7 současně ukazuje jednu z možností získání výroků z výrokových forem. Výroky ale vznikají z výrokových forem také při vázání proměnných pomocí kvantifikátorů. Všimněme si nejdříve výrokových forem s jednou proměnnou.

**Definice 1.8** Obecný výrok *příslušný k dané výrokové formě o jedné proměnné je výrok, který je pravdivý právě tehdy, vznikne-li po dosazení libovolné konstanty z oboru proměnnosti za proměnnou z této výrokové formy pravdivý výrok.*

Je-li $V(x)$ výroková forma obsahující jedinou proměnnou $x$, potom obecný výrok příslušný k této formě označíme $\forall x(V(x))$ a čteme jej „Pro každé $x$ platí $V(x)$."

Symbol $\forall x$ nazýváme *obecný kvantifikátor*. Je-li $a$ konstanta z oboru proměnnosti proměnné $x$ potom $V(a)$ označuje výrok vzniklý dosazením konstanty $a$ za $x$ do $V(x)$.

**Definice 1.9** Existenční výrok *příslušný k dané výrokové formě $V(x)$ je výrok, který je pravdivý právě tehdy, existuje-li alespoň jedna konstanta $a$ z oboru proměnnosti taková, že $V(a)$ je pravdivý výrok.*

Existenční výrok označujeme $\exists x(V(x))$ a čteme jej „Existuje alespoň jedno $x$ takové, že platí $V(x)$." Symbol $\exists x$ se nazývá *existenční kvantifikátor*.

`Poznámka:` Obecný výrok $\forall x(V(x))$ bývá také někdy zapisován ve tvaru $\forall x; V(x)$. Podobně existenční výrok $\exists x(V(x))$ se někdy zapisuje jako $\exists x; V(x)$.

**Příklad 1.11** Uvažujme výrokovou formu

$$x \geq 5 \wedge x \text{ je prvočíslo},$$

kde oborem proměnnosti proměnné $x$ je množina $\mathbb{N}$.

Zřejmě obecný výrok

$$\forall x(x \geq 5 \wedge x \text{ je prvočíslo})$$

je nepravdivý, zatímco existenční výrok

$$\exists x(x \geq 5 \wedge x \text{ je prvočíslo})$$

je pravdivý.

Uvažujeme-li nyní obecně výrokovou formu $V(x, y, \dots, z)$ o proměnných $x, y, \dots, z$, potom analogicky můžeme získat z $V(x, y, \dots, z)$ výroky, budeme-li každou z proměnných $x, y, \dots, z$ vázat pomocí některého z kvantifikátorů. Např. pro výrokové formy o dvou proměnných existuje celkem 8 možností, jak vázat proměnné pomocí kvantifikátorů. Je-li $V(x, y)$ výroková forma, pak získáme výroky

$$\forall x \forall y (V(x, y))$$

$$\forall y \forall x (V(x, y))$$

$$\forall x \exists y (V(x, y))$$

$$\exists y \forall x (V(x, y))$$

$$\exists x \forall y (V(x, y))$$

$$\forall y \exists x (V(x, y))$$

$$\exists x \exists y (V(x, y))$$

$$\exists y \exists x (V(x, y))$$

**Příklad 1.12** Uvažujeme výrokovou formu $y = x + 1$, kde $x, y$ jsou libovolná přirozená čísla. Zapíšeme všech 8 výroků, které dostaneme z této výrokové formy pomocí kvantifikátorů a určíme jejich pravdivostní hodnoty.

$$\forall x \forall y (y = x + 1) \dots 0$$

$$\forall y \forall x (y = x + 1) \dots 0$$

$$\forall x \exists y (y = x + 1) \dots 1$$

$$\exists y \forall x (y = x + 1) \dots 0$$

$$\exists x \forall y (y = x + 1) \dots 0$$

$$\forall y \exists x (y = x + 1) \dots 0$$

$$\exists x \exists y (y = x + 1) \dots 1$$

$$\exists y \exists x (y = x + 1) \dots 1$$

V příkladu 1.12 platí, že při použití jenom obecných nebo jenom existenčních kvantifikátorů jsme dostali stejné pravdivostní hodnoty bez ohledu na pořadí kvantifikátorů, zatímco pro pořadí kvantifikátorů $\forall x \exists y$ a $\exists y \forall x$ jsou pravdivostní hodnoty různé. Platí také obecně, že vážeme-li ve výrokové formě $V(x, y, \dots, z)$ všechny proměnné $x, y, \dots, z$ buď jen pomocí obecných nebo jen pomocí existenčních kvantifikátorů, nezáleží pravdivostní hodnoty vzniklých výroků na pořadí užitých kvantifikátorů. Ovšem při použití různých typů kvantifikátorů je jejich pořadí podstatné, jak je vidět v příkladu 1.12.

Při práci s matematickými pojmy a větami bude často zapotřebí vytvářet negace výrazů, ve kterých se vyskytují kvantifikátory. Musíme proto vědět, jak s takovými výrazy pracovat.

Předpokládejme nejdříve, že $V(x)$ je výroková forma o jedné proměnné $x$ a že proměnná $x$ může nabývat konečného počtu hodnot $a_1, a_2, \ldots, a_n$. Potom obecný výrok $\forall x(V(x))$ je pravdivý právě tehdy, když je pravdivá konjunkce

$$V(a_1) \wedge V(a_2) \wedge \ldots \wedge V(a_n),$$

podobně existenční výrok $\exists x(V(x))$ je pravdivý právě tehdy, když je pravdivá disjunkce

$$V(a_1) \vee V(a_2) \vee \ldots \vee V(a_n),$$

Použitím de Morganových pravidel tedy dostáváme následující pravdivé ekvivalence:

$$\neg[\forall x(V(x))] \Leftrightarrow \neg[V(a_1) \wedge V(a_2) \wedge \ldots \wedge V(a_n)] \Leftrightarrow$$

$$\Leftrightarrow [\neg V(a_1) \vee \neg V(a_2) \vee \ldots \vee \neg V(a_n)] \Leftrightarrow \exists x[\neg V(x)],$$

$$\neg[\exists x(V(x))] \Leftrightarrow \neg[V(a_1) \vee V(a_2) \vee \ldots \vee V(a_n)] \Leftrightarrow$$

$$\Leftrightarrow [\neg V(a_1) \wedge \neg V(a_2) \wedge \ldots \neg \wedge V(a_n)] \Leftrightarrow \forall x(\neg V(x)).$$

Proto jsou v tomto případě pravdivé ekvivalence

$$\neg[\forall x(V(x))] \Leftrightarrow \exists x(\neg V(x)) \text{ a}$$

$$\neg[\exists x(V(x))] \Leftrightarrow \forall x(\neg V(x)).$$

Tyto ekvivalence jsou však pravdivé i pro výrokové formy s nekonečnými obory proměnnosti svých proměnných, proto je můžeme používat zcela obecně.

Pokud výroková forma $V(x, y, \ldots, z)$ obsahuje proměnné $x, y, \ldots, z$ a uvažujeme-li některý z výroků, který vznikl z této formy vázáním každé z proměnných některým kvantifikátorem, pak negace takového výroku je logicky ekvivalentní s výrokem, který vznikne z původního výroku záměnou všech obecných kvantifikátorů existenčními a naopak a záměnou výrokové formy $V(x, y, \ldots, z)$ její negací $\neg V(x, y, \ldots, z)$.

**Příklad 1.13** Pro výrokovou formu $x \leq y$, kde $x, y$ patří do $\mathbb{N}$, jsou např. pravdivé ekvivalence

$$\neg[\forall x \exists y(x \leq y)] \Leftrightarrow \exists x \forall y(\neg(x \leq y)),$$

tj.

$$\neg[\forall x \exists y(x \leq y)] \Leftrightarrow \exists x \forall y((x > y)),$$

popř.

$$\neg[\exists y \exists x(x \leq y)] \Leftrightarrow \forall y \forall x(\neg(x \leq y)), \text{ apod.}$$

## 1.4 Důkazy matematických vět

Většina vět, které se v matematice vyskytují, je ve tvaru implikace nebo ekvivalence. Zaveďme si některé pojmy, které se týkají právě vět ve tvaru implikace.

**Definice 1.10** *Jsou-li $\mathcal{A}, \mathcal{B}$ libovolné formule některé teorie, pak*

*a) větu $\mathcal{B} \Rightarrow \mathcal{A}$ nazýváme* obrácenou větou *k větě $\mathcal{A} \Rightarrow \mathcal{B}$;*

*b) větu $\neg\mathcal{B} \Rightarrow \neg\mathcal{A}$ nazýváme* obměněnou větou *(nebo také* kontraponovanou větou*) k větě $\mathcal{A} \Rightarrow \mathcal{B}$.*

Obecně platí, že dosadíme-li do některé tautologie výrokového počtu za výrokové proměnné libovolné formule dané teorie (ovšem za stejné proměnné vždy stejné formule), dostaneme pravdivé tvrzení té teorie. Proto na základě tautologie

$$(A \Leftrightarrow B) \Leftrightarrow [(A \Rightarrow B) \wedge (B \Rightarrow A)]$$

platí, že pro libovolné formule $\mathcal{A}$ a $\mathcal{B}$ jsou logicky ekvivalentní věty $\mathcal{A} \Leftrightarrow \mathcal{B}$ a $(\mathcal{A} \Rightarrow \mathcal{B}) \wedge (\mathcal{B} \Rightarrow \mathcal{A})$. Tedy dokazování věty $\mathcal{A} \Leftrightarrow \mathcal{B}$ je ekvivalentní s dokazováním dvou vět: věty $\mathcal{A} \Rightarrow \mathcal{B}$ a věty k ní obrácené $\mathcal{B} \Rightarrow \mathcal{A}$.

Podobně podle tautologie

$$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$$

platí, že věta $\mathcal{A} \Rightarrow \mathcal{B}$ je logicky ekvivalentní s větou obměněnou, takže dokázat větu $\mathcal{A} \Rightarrow \mathcal{B}$ je totéž, jako dokázat větu $\neg\mathcal{B} \Rightarrow \neg\mathcal{A}$.

Ukažme nyní, jakých metod používáme při dokazování vět ve tvaru implikace.

*Přímý důkaz*: Víme, že je tautologií formule

$$[(A \Rightarrow B) \wedge (B \Rightarrow C)] \Rightarrow (A \Rightarrow C).$$

Indukcí snadno ověříme, že také jsou-li $A_1, A_2, \ldots, A_n$, kde $n \geq 2$, výrokové proměnné, pak je tautologií formule

$$[(A_1 \Rightarrow A_2) \wedge (A_2 \Rightarrow A_3) \wedge \ldots \wedge (A_{n-1} \Rightarrow A_n)] \Rightarrow (A_1 \Rightarrow A_n).$$

Bude tedy platit, že jsou-li $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n$ $(n \geq 2)$ formule a dokážeme-li věty $\mathcal{A}_1 \Rightarrow \mathcal{A}_2, \mathcal{A}_2 \Rightarrow \mathcal{A}_3, \ldots, \mathcal{A}_{n-1} \Rightarrow \mathcal{A}_n$, dokázali jsme tím také větu $\mathcal{A}_1 \Rightarrow \mathcal{A}_n$. Tuto metodu důkazu budeme s výhodou používat, můžeme-li důkaz dané věty rozdělit na postupné dokazování elementárnějších kroků.

**Příklad 1.14** Dokažte větu: Je-li $U$ vnitřní bod trojúhelníka $ABC$, pak platí

$$|AU| + |BU| + |CU| > s,$$

kde $s$ je polovina obvodu trojúhelníka $ABC$.

Pro důkaz označme výroky:

($\mathcal{A}$) $U$ je vnitřní bod trojúhelníka $ABC$.

($\mathcal{A}_2$) $U$ neleží na žádné ze stran $AB, BC, CA$.

($\mathcal{A}_3$) Pro body $A, B, C, U$, platí

$$|AU| + |BU| > |AB|,$$
$$|AU| + |CU| > |AC|,$$
$$|BU| + |CU| > |BC|.$$

($\mathcal{B}$) Pro body $A, B, C, U$ platí

$$|AU| + |BU| + |CU| > s.$$

Máme tedy dokázat větu $\mathcal{A} \Rightarrow \mathcal{B}$. Položíme-li $\mathcal{A}_1 = \mathcal{A}$, $\mathcal{A}_4 = \mathcal{B}$, pak jsou zřejmě pravdivé věty

$$\mathcal{A}_1 \Rightarrow \mathcal{A}_2, \mathcal{A}_2 \Rightarrow \mathcal{A}_3, \mathcal{A}_3 \Rightarrow \mathcal{A}_4,$$

a proto bude pravdivá i věta $\mathcal{A}_1 \Rightarrow \mathcal{A}_4$.

Zvláštním případem přímého důkazu je důkaz matematickou indukcí, který využívá následující vlastnosti množiny všech přirozených čísel $\mathbb{N}$:

Nechť $V(x)$ je výroková forma, kde oborem proměnnosti je množina $\mathbb{N}$. Je-li pro některé přirozené číslo $n_0$ pravdivý výrok $V(n_0)$ a vyplývá-li pro každé přirozené číslo $k \geq n_0$ z pravdivosti výroku $V(k)$ také pravdivost výroku $V(k+1)$, potom je pravdivý výrok pro každé přirozené číslo $n \geq n_0$.

**Příklad 1.15** Dokažte, že pro každé přirozené číslo $n \geq 3$ platí $2^n > 2n$.

Označme $V(x) = (2^x > 2x)$. Platí

$$8 = 2^3 > 2 \cdot 3 = 6,$$

tedy výrok $V(3)$ je pravdivý.

Předpokládejme, že je pravdivý výrok $V(k)$, kde $k \geq 3$ je přirozené číslo. Potom platí

$$2^{k+1} = 2^k \cdot 2 > 2k \cdot 2 = 2k + 2k > 2k + 2 = 2(k+1),$$

tedy je pravdivý také výrok $V(k+1)$. Proto $V(n)$ je pravdivý výrok pro každé přirozené číslo $n \geq 3$.

*Důkaz sporem*: Předpokládejme, že $A$ a $B$ jsou výrokové proměnné, $\mathcal{K}$ je některá kontradikce. Jestliže pro některé dosazení pravdivostních hodnot za výrokové proměnné je výrok

$$(A \wedge \neg B) \Rightarrow \mathcal{K}$$

pravdivý, pak (protože $\mathcal{K}$ je vždy nepravdivá) konjunkce $A \wedge \neg B$ musí být pro toto dosazení nepravdivá. Tedy je pravdivý výrok $\neg(A \wedge \neg B)$, který je ale ekvivalentní s výrokem $A \Rightarrow B$. (Podle tautologií $\neg(A \Rightarrow B) \Leftrightarrow (A \wedge \neg B)$ a $\neg\neg A \Leftrightarrow A$). Proto jsou-li $\mathcal{A}$ a $\mathcal{B}$ libovolné formule a dojdeme-li za předpokladu $\mathcal{A} \wedge \neg \mathcal{B}$ ke sporu s některou již dokázanou skutečností, pak je pravdivá formule $\mathcal{A} \Rightarrow \mathcal{B}$.

**Příklad 1.16** Dokažte, že jsou-li $\alpha$ a $\beta$ libovolná komplexní čísla, pak $|\alpha+\beta| \leq |\alpha|+|\beta|$.
Označme výroky:

($\mathcal{A}$) $\alpha$ a $\beta$ jsou komplexní čísla.

($\mathcal{B}$) $|\alpha+\beta| \leq |\alpha|+|\beta|$.

Předpokládejme, že je pravdivý výrok $\mathcal{A} \wedge \neg\mathcal{B}$, tzn., že $\alpha$ a $\beta$ jsou komplexní čísla a přitom $|\alpha|+|\beta| < |\alpha+\beta|$. Tedy platí-li $\alpha = a_1 + a_2 i$, $\beta = b_1 + b_2 i$ ($a_1, a_2, b_1, b_2$ jsou reálná čísla), potom podle předpokladu

$$\sqrt{a_1^2 + a_2^2} + \sqrt{b_1^2 + b_2^2} < \sqrt{(a_1+b_1)^2 + (a_2+b_2)^2}.$$

Po snadných úpravách dojdeme k nerovnostem

$$(a_1 b_2 - a_2 b_1)^2 < 0,$$

a to je spor s vlastnostmi druhých mocnin reálných čísel. Musí tedy platit věta $\mathcal{A} \Rightarrow \mathcal{B}$, kterou jsme chtěli dokázat.

## 1.5 Cvičení

**1.1** Zjistěte, je-li výraz
a) $(B \Rightarrow \neg(A \wedge (C \vee \neg B)) \Leftrightarrow (\neg(B \wedge A))$;
b) $\neg(A \Rightarrow \neg C) \Leftrightarrow (B \Rightarrow (C \Leftrightarrow \neg A))$
formulí výrokové logiky.
[ a) ano; b) ne ]

**1.2** Zjistěte, zda platí distributivita implikace vzhledem k ekvivalenci, tzn.

$$[X \Rightarrow (Y \Leftrightarrow Z)] \Leftrightarrow [(X \Rightarrow Y) \Leftrightarrow (X \Rightarrow Z)].$$

[ ano ]

**1.3** Rozhodněte zda je daná formule tautologie:
a) $\neg(A \Rightarrow B) \Leftrightarrow (A \wedge \neg B)$;
b) $\neg(A \wedge B \wedge C) \Leftrightarrow (\neg A \vee \neg B \vee \neg C)$;
c) $\neg(A \wedge B) \Leftrightarrow (\neg A \wedge \neg B)$;
d) $[(A \Rightarrow \neg B) \Rightarrow (\neg C \vee B)] \Leftrightarrow [(\neg B \wedge C) \Rightarrow (B \wedge A)]$;
e) $(A \Rightarrow C) \Rightarrow [(A \Rightarrow B) \Rightarrow (B \Rightarrow C)]$.
[ a) ano; b) ano; c) ne; d) ano; e) ne ]

**1.4** Na základě výrokové logiky ověřte, zda následující úsudek je správný. Viníkem je Petr nebo Pavel. Je-li viníkem Petr, pak Pavel nebyl v 11 hodin na místě činu. Je-li viníkem Pavel, pak je jasný motiv činu. Tedy, jestliže byl Pavel v 11 hodin na místě činu, pak je jasný motiv činu.
[ ano ]

**1.5** Zapište všechny výroky, které lze získat z dané výrokové formy vázáním proměnných kvantifikátory, a určete jejich pravdivostní hodnoty:

a) $x \leq y \quad (x, y \in \mathbb{N})$;

b) $x \leq y \quad (x, y \in \mathbb{Z})$;

c) $x^2 + y \geq 2 \quad (x \in \mathbb{R}, y \in \mathbb{N})$.

**1.6** Vytvořte k dané větě obrácenou větu, obměněnou větu a negaci a rozhodněte o pravdivosti nebo nepravdivosti každé z těchto čtyř vět:

a) $\forall x \in \mathbb{Z}; (4 \text{ dělí } x \wedge 3 \text{ dělí } x) \Rightarrow 12 \text{ dělí } x$;

b) $\forall x \forall y (x - y \neq 0 \Rightarrow x^2 - y^2 \neq 0) \ (x, y \in \mathbb{C})$;

c) $\forall x \forall y (x < y \Rightarrow \exists z \ (x + z = y)) \ (x, y, z \in \mathbb{N})$.

**1.7** Dokažte pomocí přímého důkazu větu:
Tvoří-li kladná čísla $a_1, a_2, \ldots, a_n$ prvních $n$ členů geometrické posloupnosti, potom

$$a_1 \cdot a_2 \cdot \ldots \cdot a_n = (a_1 \cdot a_n)^n.$$

**1.8** Dokažte sporem větu:

a) Jestliže $ax_1 + b \neq ax_2 + b \ (a, b, x_1, x_2 \in \mathbb{R}, a \neq 0)$, pak $x_1 \neq x_2$;

b) Každá posloupnost reálných čísel má nejvýše jednu limitu.

c) Daným bodem nelze vést k dané přímce dvě různé kolmice.

**1.9** Dokažte matematickou indukcí, že pro každé $n \in \mathbb{N}$ platí:

a) $1 + 3 + 5 + \cdots + (2n - 1) = n^2$;

b) $1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{1}{4}n^2(n + 1)^2$;

c) $1 + 3^1 + 3^2 + \cdots + 3^n = \frac{3^{n+1}-1}{2}$;

d) $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n\cdot(n+1)} = \frac{n}{n+1}$;

e) Číslo $n^3 + 5n$ je dělitelné šesti.

f) $\cos\alpha + \cos 3\alpha + \cdots + \cos(2n - 1)\alpha = \frac{\sin 2n\alpha}{2\sin\alpha}, \ \sin\alpha \neq 0$.

**1.10** Určete, pro která $n \in \mathbb{N}$ platí:

a) $2^n > 2n + 1$;

b) Číslo $n^3 - n$ je dělitelné šesti.
[ a) $n \geq 3$; b) $n \geq 1$ ]

**1.11** Určete počet úhlopříček pravidelného $n$-úhelníku a své tvrzení dokažte matematickou indukcí.
[ $\frac{1}{2}n(n-3)$ ]

# Kapitola 2

# Množiny, relace, zobrazení

## 2.1 Pojem množiny

Základním pojmem, se kterým pracuje současná matematika, je pojem *množiny*. Intuitivně je množina chápána jako jakýkoliv soubor jakýchkoliv objektů (*prvků*). Pojem „soubor“ se už blíže neurčuje.

K zápisům množin budeme používat velká písmena $A, B, \ldots, X, \ldots$, prvky množin budeme zpravidla značit malými písmeny $a, b, \ldots, x, y, \ldots$. Výrok „$x$ je prvkem $A$“ označíme symbolicky $x \in A$. Pokud $x$ není prvkem $A$, používáme označení $x \notin A$. Množiny, které obsahují konečný počet prvků, se nazývají *konečné*, ostatní množiny jsou *nekonečné*. Zvláštním případem množiny je *prázdná množina*, která neobsahuje žádné prvky. Prázdnou množinu označíme symbolem $\emptyset$. Víme-li, že do množiny $A$ patří právě všechny prvky $x_1, x_2, \ldots$, pak píšeme také $A = \{x_1, x_2, \ldots\}$. S výhodou používáme takového zápisu pro konečné množiny. Je-li $V(x)$ výroková forma o jedné proměnné a je-li $P$ obor proměnnosti proměnné $x$, pak $A = \{x \in P; V(x)\}$ označuje množinu, která se skládá právě ze všech prvků $a$ z oboru proměnnosti $P$, pro které je $V(a)$ pravdivým výrokem. Říkáme pak také, že množina $A$ je určena pomocí *charakteristické vlastnosti* $V$. Je-li znám obor proměnnosti $P$, pak můžeme také psát zkráceně $A = \{x; V(x)\}$.

**Příklad 2.1**

a) Nechť $A$ je množina všech kořenů rovnice $x^2 - x - 6 = 0$. Pak množinu $A$ můžeme také zapsat pomocí jejích prvků ve tvaru $A = \{-2, 3\}$

b) Pomocí prvků můžeme zapsat také některé nekonečné množiny, např. $\mathbb{N} = \{1, 2, \ldots\}$ bude množina všech přirozených čísel, $\{0, -1, -2, \ldots\}$ je množina všech celých nekladných čísel, apod.

c) U nekonečných množin často s výhodou používáme zápisů pomocí charakteristických vlastností. Např. $B = \{x \in \mathbb{Z}; x > \sqrt{20}\}$ značí množinu všech celých čísel, která jsou větší nebo rovna číslu 5.

Samozřejmě pomocí charakteristické vlastnosti můžeme popisovat i konečné množiny.

Pro množinu $A$ z části a) platí $A = \{x \in \mathbb{Z}; x^2 - x - 6 = 0\}$. Označíme-li $C = \{x \in \mathbb{Z}; 4x^2 + 9 = 0\}$, pak C je prázdná množina.

`Poznámka:` Uvědomme si ale, že zavedení pojmu množina pomocí pojmu „soubor prvků“ nemůžeme považovat za definici. Ukážeme si tuto skutečnost pomocí tzv. *Russelova paradoxu.*

Všechny množiny si rozdělíme do dvou skupin. Do první skupiny zařadíme všechny takové množiny, které nejsou svými prvky. Množiny z této skupiny nazveme *normální*. Všechny množiny, které nejsou normální, zařadíme do druhé skupiny. (Normální množinou je např. množina všech obyvatel ČR, zatímco množina všech množin není normální.) Označme symbolem $A$ množinu všech normálních množin, tj. $A = \{X; X \notin X\}$. Předpokládejme, že množina $A$ je normální, jinými slovy $A$ patří do množiny všech normálních množin, tj. $A \in A$. Pak však $A$ má vlastnost, pomocí níž je definována množina všech normálních množin, tzn. $A \notin A$. Předpokládejme proto, že $A$ není normální. Pak $A$ nepatří do množiny všech normálních množin, tj. $A \notin A$. To však znamená, že $A$ má vlastnost, pomocí níž je určena množina všech normálních množin, tedy $A \in A$. Zjistili jsme tak, že $A$ je i není normální současně, což není možné.

Podobných paradoxů, jako je Russelův paradox bychom mohli najít velké množství. Všechny tyto paradoxy mají původ v tom, že chápání množiny jako souboru prvků umožňuje uvažovat i tak „velké“ množiny, jako je množina všech množin. Proto je zapotřebí při studiu množin postupovat axiomaticky tak, aby se podobné paradoxy nevyskytovaly. (V průběhu studia v dalších semestrech se axiomatickým přístupem k teorii množin budeme podrobně zabývat.)

Pro naše účely však zatím bude postačovat intuitivní přístup k pojmu množina, protože paradoxům se také vyhneme, budeme-li všechny zkoumané množiny vybírat jako části některé tzv. *univerzální množiny* $\mathcal{U}$.

## 2.2 Operace s množinami

Připomeňme si ještě jednou, že všechny množiny, které budeme uvažovat, jsou částmi některé univerzální množiny .

**Definice 2.1** Průnikem *množin $A$ a $B$ rozumíme množinu* $A \cap B = \{x; x \in A \wedge x \in B\}$.

**Definice 2.2** Sjednocení *množin $A$ a $B$ je množina* $A \cup B = \{x; x \in A \vee x \in B\}$.

**Definice 2.3**

*a)* Rozdílem *množin $A$ a $B$ (v tomto pořadí) nazýváme množinu* $A \setminus B = \{x; x \in A \wedge x \notin B\}$.

*b) Rozdíl $A' = \mathcal{U} \setminus A$ se také nazývá* doplněk *množiny $A$.*

**Příklad 2.2** Nechť $A$ je množina všech sudých přirozených čísel, $B$ množina všech přirozených prvočísel. Potom $A \cup B$ je množina všech takových přirozených čísel, která jsou různá od čísla 1 a od všech lichých složených čísel, $A \cap B$ je jednoprvková množina $\{2\}$, $A \setminus B$ je množina všech sudých přirozených čísel větších než 2 a $B \setminus A$ je množina všech přirozených lichých prvočísel.

**Definice 2.4** *Množina $A$ se nazývá podmnožinou množiny $B$ (značíme $A \subseteq B$), jestliže*

$$\forall x(x \in A \Rightarrow x \in B).$$

*Jestliže $A \subseteq B$ a množina $A$ je různá od množiny $B$, pak říkáme, že $A$ je* vlastní podmnožinou *množiny $B$ a značíme $A \subset B$.*

Vztah „být podmnožinou“ nazýváme *množinová inkluze*.

**Definice 2.5** *Řekneme, že množina $A$* se rovná množině *$B$, jestliže*

$$\forall x(x \in A \Leftrightarrow x \in B).$$

Vidíme tedy, že množina $A$ se rovná množině $B$ tehdy jen tehdy, je-li $A$ podmnožinou $B$ a současně $B$ je podmnožinou $A$. Této skutečnosti budeme také při důkazech rovnosti dvou množin často využívat.

**Věta 2.1** *Jsou-li $A, B, C$ množiny, pak platí*

*a)* $A = A$, *(reflexivnost)*

*b)* $A = B \Rightarrow B = A$, *(symetričnost)*

*c)* $(A = B \wedge B = C) \Rightarrow A = C$. *(tranzitivnost)*

**Věta 2.2** *Pro libovolné množiny $A, B, C$ platí*

*a)* $A \subseteq A$, *(reflexivnost)*

*b)* $(A \subseteq B \wedge B \subseteq A) \Rightarrow A = B$, *(antisymetričnost)*

*c)* $(A \subseteq B \wedge B \subseteq C) \Rightarrow A \subseteq C$. *(tranzitivnost)*

Důkazy obou těchto vět jsou zřejmé. Ukažme si další potřebné vlastnosti zavedených pojmů.

**Věta 2.3** *Pro libovolné množiny $A, B, C$ platí*

*a)* $A \cap B = B \cap A$, $A \cup B = B \cup A$, *(komutativita)*

*b)* $A \cap (B \cap C) = (A \cap B) \cap C$, $A \cup (B \cup C) = (A \cup B) \cup C$ *(asociativita)*

*c)* $A \cap A = A$, $A \cup A = A$, *(idempotentnost)*

*d)* $A \cap \emptyset = \emptyset$, $A \cup \emptyset = A$,

*e)* $A \cap \mathcal{U} = A$, $A \cup \mathcal{U} = \mathcal{U}$,

*f)* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(distributivita)* *g)* $A \setminus \emptyset = A$, $A \setminus \mathcal{U} = \emptyset$, $\emptyset \setminus A = \emptyset$, $A \setminus A = \emptyset$, $\mathcal{U} \setminus A = A'$,

*h)* $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$, $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$, $(A \cap B)' = (A' \cup B')$, $(A \cup B)' = (A' \cap B')$.

`Poznámka`: Podle vlastností a) jsou průnik i sjednocení komutativní, podle b) jsou asociativní, c) je vyjádřením toho, že průnik a sjednocení jsou idempotentní, podle f) je průnik distributivní vzhledem ke sjednocení a sjednocení je distributivní vzhledem k průniku. Vlastnosti h) se nazývají (analogicky jako odpovídající tautologie) de Morganovy zákony.

D ů k a z: Dokažme jenom první z rovností v částech f) a h) . Zbývající rovnosti si čtenář snadno ověří sám.

f) Nechť $A, B, C$ jsou množiny. Pak

$$x \in A \cap (B \cup C) \Leftrightarrow (x \in A \wedge x \in B \cup C) \Leftrightarrow [x \in A \wedge (x \in B \vee x \in C)] \Leftrightarrow$$
$$\Leftrightarrow [(x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)] \Leftrightarrow (x \in A \cap B \vee x \in A \cap C) \Leftrightarrow$$
$$\Leftrightarrow x \in (A \cap B) \cup (A \cap C),$$

tedy podle definice rovnosti množin platí

$$[A \cap (B \cup C)] = (A \cap B) \cup (A \cap C).$$

(V důkazu jsme využívali definice 2.1 a 2.2 a distributivnost konjunkce vzhledem k disjunkci.)

h) Jsou-li $A, B, C$ množiny, pak platí

$$x \in C \setminus (A \cap B) \Leftrightarrow (x \in C \wedge x \notin A \cap B) \Leftrightarrow [x \in C \wedge \neg(x \in A \cap B)] \Leftrightarrow$$
$$\Leftrightarrow [x \in C \wedge \neg(x \in A \wedge x \in B)] \Leftrightarrow [x \in C \wedge (x \notin A \vee x \notin B)] \Leftrightarrow$$
$$\Leftrightarrow [(x \in C \wedge x \notin A) \vee (x \in C \wedge x \notin B)] \Leftrightarrow (x \in C \setminus A \vee x \in C \setminus B) \Leftrightarrow$$
$$\Leftrightarrow x \in (C \setminus A) \cup (C \setminus B),$$

tzn., že

$$[C \setminus (A \cap B)] = (C \setminus A) \cup (C \setminus B)$$

(Použili jsme definici 2.3, de Morganův zákon a distributivní zákon výrokové logiky a definici 2.5.)

$\square$

**Věta 2.4** *Pro každé množiny A a B platí*

$$A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B.$$

$\square$

Nyní si zaveďme ještě jednu operaci s množinami:

**Definice 2.6** *Jsou-li $A$ a $B$ množiny, pak jejich* kartézským součinem *(v tomto pořadí) rozumíme množinu*

$$A \times B = \{x = (a, b); a \in A \wedge b \in B\}.$$

*($(a, b)$ znamená uspořádanou dvojici prvků $a$ a $b$.)*

Kartézský součin $A \times A$ značíme také $A^2$ a nazýváme *kartézský čtverec* neboli *kartézská mocnina* (druhá) množiny $A$.

**Příklad 2.3** Jestliže $A = \{1, 2, 3\}, B = \{a, b\}$, pak

$$A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\},$$

$$B \times A = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}.$$

`Poznámka:` Jsou-li $A_1, \ldots, A_n$ množiny, pak můžeme analogicky zavést pojem *kartézského součinu* $A_1 \times \ldots \times A_n$ těchto množin jako množinu všech uspořádaných $n$-tic

$$(a_1, \ldots, a_n), \text{ kde } a_1 \in A_1, \ldots, a_n \in A_n.$$

Dále pro množinu $A$ budeme rozumět *$n$-tou kartézskou mocninou* ($n \geq 1$) této množiny množinu $A^n = \underbrace{A \times \ldots \times A}_{n\text{-krát}}$.

Ukažme si nyní, jaký je vztah mezi operací kartézského součinu a operacemi sjednocení, průniku a rozdílu množin.

**Věta 2.5** *Pro každé množiny $A, B, C$ platí*

*a)* $C \times (A \cap B) = (C \times A) \cap (C \times B)$,

*b)* $C \times (A \cup B) = (C \times A) \cup (C \times B)$,

*c)* $C \times (A \setminus B) = (C \times A) \setminus (C \times B)$.

D ů k a z:

a) $x = (a, b) \in C \times (A \cap B) \Leftrightarrow (a \in C \wedge b \in A \cap B) \Leftrightarrow [a \in C \wedge (b \in A \wedge b \in B)] \Leftrightarrow [(a \in C \wedge a \in C) \wedge (b \in A \wedge b \in B)] \Leftrightarrow [(a, b) \in C \times A \wedge (a, b) \in C \times B] \Leftrightarrow x = (a, b) \in (C \times A) \cap (C \times B)$ (V důkazu jsme použili definice 2.6 a 2.1 a idempotentnost, komutativnost a asociativnost logické operace konjunkce výroků.)

b) $x = (a, b) \in C \times (A \cup B) \Leftrightarrow (a \in C \wedge b \in A \cup B) \Leftrightarrow [a \in C \wedge (b \in A \vee b \in B)] \Leftrightarrow [(a \in C \wedge b \in A) \vee (a \in C \wedge b \in B)] \Leftrightarrow [(a, b) \in C \times A \vee (a, b) \in C \times B] \Leftrightarrow x = (a, b) \in (C \times A) \cup (C \times B)$

c) $x = (a, b) \in C \times (A \setminus B) \Leftrightarrow (a \in C \wedge b \in A \setminus B) \Leftrightarrow [a \in C \wedge (b \in A \wedge b \notin B)] \Leftrightarrow [(a \in C \wedge a \in C) \wedge (b \in A \wedge b \notin B)] \Leftrightarrow [(a \in C \wedge b \in A) \wedge (a \in C \wedge b \notin B)] \Leftrightarrow [(a, b) \in C \times A \wedge (a, b) \notin C \times B] \Leftrightarrow x = (a, b) \in (C \times A) \setminus (C \times B)$

$\square$

## 2.3 Binární relace

Připomeňme si nyní pojem binární relace, se kterým jste se již setkali na střední škole.

**Definice 2.7** Binární relací mezi množinami $A$ *a* $B$ *(v tomto pořadí) nazýváme libovolnou podmnožinu* $\rho$ *kartézského součinu* $A \times B$.

Jestliže $\rho \subseteq A^2$, pak se $\rho$ nazývá také *binární relace na množině* $A$.

`Poznámka:` Jestliže $a \in A, b \in B$, pak skutečnost, že $(a, b) \in \rho$, budeme někdy také zapisovat ve tvaru $a\rho b$. Zejména u konkrétních běžně používaných relací je tento způsob zápisu obvyklý. Např. je-li „$<$“ relace „menší než“ na množině všech přirozených čísel, pak místo $(a, b) \in <$ píšeme $a < b$.

Protože je každá binární relace vlastně množina, nemusíme zvláště definovat pojmy sjednocení, průniku, rozdílu, popř. doplňku relací. Ovšem binární relace jsou specifickým případem množin, a proto můžeme zavést ještě další operace s binárními relacemi.

**Definice 2.8** *Je-li* $\rho \subseteq A \times B$ *binární relace mezi množinami* $A$ *a* $B$, *pak* inverzní relací *k relaci* $\rho$ *rozumíme binární relaci mezi množinami* $B$ *a* $A$ *(*$\rho^{-1} \subseteq B \times A$*) takovou, že*

$$\forall a \in A, b \in B; (b, a) \in \rho^{-1} \Leftrightarrow (a, b) \in \rho.$$

**Příklad 2.4**

a) Jsou-li $A = \{a, b, c\}$, $B = \{1, 2, 3\}$, $\rho = \{(a, 2), (b, 1), (a, 1), (c, 2), (c, 3)\}$ pak $\rho^{-1} = \{(2, a), (1, b), (1, a), (2, c), (3, c)\}$.

b) Pro relaci „$<$“ na množině všech přirozených čísel $\mathbb{N}$ platí $<^{-1} = >$.

**Definice 2.9** *Nechť* $\rho \subseteq A \times B$, $\sigma \subseteq B \times C$. *Potom* složením binárních relací $\rho$ a $\sigma$ *(v tomto pořadí) nazýváme binární relaci* $\rho \circ \sigma$ *mezi množinami* $A$ *a* $C$ *(*$\rho \circ \sigma \subseteq A \times C$*) takovou, že*

$$\forall a \in A, c \in C; (a, c) \in \rho \circ \sigma \Leftrightarrow (\exists b \in B; (a, b) \in \rho \wedge (b, c) \in \sigma).$$

**Příklad 2.5**

a) Jestliže $A = \{a, b, c, d\}$, $B = \{1, 2, 3\}$, $C = \{\alpha, \beta, \gamma\}$, $\rho \subseteq A \times B$, $\sigma \subseteq B \times C$, $\rho = \{(a, 2), (b, 1), (a, 3), (c, 1), (d, 2), (b, 3)\}$, $\sigma = \{(1, \beta), (1, \gamma), (2, \alpha), (2, \gamma), (3, \alpha)\}$, pak

$$\rho \circ \sigma = \{(a, \alpha), (a, \gamma), (b, \beta), (b, \gamma), (c, \beta), (c, \gamma), (d, \alpha), (d, \gamma), (b, \alpha)\}.$$

Přitom relace $\sigma \circ \rho$ neexistuje. (Přesněji: $\sigma \circ \rho$ je prázdná relace.)

b) Uvažujme relace „$<$“ a „$>$“ na množině všech přirozených čísel $\mathbb{N}$. Jsou-li $x, y \in \mathbb{N}$, pak

$$(x, y) \in < \circ > \Leftrightarrow (\exists z \in \mathbb{N}; x < z \wedge z > y) \Leftrightarrow (\exists z \in \mathbb{N};\ \max\{x, y\} < z),$$

tedy $<\circ> = \mathbb{N}^2$ a

$$(x,y) \in > \circ < \Leftrightarrow (\exists u \in \mathbb{N}; x > u \wedge u < y) \Leftrightarrow (\exists u \in \mathbb{N}; u < \min\{x,y\}),$$

tedy $> \circ < = \{(x,y) \in \mathbb{N}^2; x > 1 \wedge y > 1\}$. Takže

$$< \circ > \neq > \circ < .$$

Na základě příkladu 2.5 vidíme, že složení binárních relací není obecně komutativní. Podle a) může existovat složení $\rho \circ \sigma$ a přitom složení $\sigma \circ \rho$ existovat nemusí a podle b) z existence obou složení $\rho \circ \sigma$ a $\sigma \circ \rho$ ještě neplyne jejich rovnost.

**Věta 2.6** *Pro libovolné binární relace $\rho \subseteq A \times B$, $\sigma \subseteq B \times C$, $\tau \subseteq C \times D$ platí*

*a)* $(\rho^{-1})^{-1} = \rho$,

*b)* $\rho \circ (\sigma \circ \tau) = (\rho \circ \sigma) \circ \tau$,

*c)* $(\rho \circ \sigma)^{-1} = \sigma^{-1} \circ \tau^{-1}$.

D ů k a z:

a) Jsou-li $a \in A, b \in B$, pak

$$(a,b) \in (\rho^{-1})^{-1} \Leftrightarrow (b,a) \in \rho^{-1} \Leftrightarrow (a,b) \in \rho,$$

tedy $(\rho^{-1})^{-1} = \rho$.

b) Nechť $a \in A, d \in D$. Pak $(a,d) \in \rho \circ (\sigma \circ \tau) \Leftrightarrow (\exists b \in B; (a,b) \in \rho \wedge (b,d) \in \sigma \circ \tau) \Leftrightarrow (\exists b \in B \exists c \in C; (a,b) \in \rho \wedge [(b,c) \in \sigma \wedge (c,d) \in \tau]) \Leftrightarrow (\exists b \in B \exists c \in C; [(a,b) \in \rho \wedge (b,c) \in \sigma] \wedge (c,d) \in \tau) \Leftrightarrow (\exists c \in C; (a,c) \in \rho \circ \sigma \wedge (c,d) \in \tau) \Leftrightarrow (a,d) \in (\rho \circ \sigma) \circ \tau$, tzn. $\rho \circ (\sigma \circ \tau) = (\rho \circ \sigma) \circ \tau$.

c) Nechť $a \in A, c \in C$. Pak $(c,a) \in (\rho \circ \sigma)^{-1} \Leftrightarrow (a,c) \in \rho \circ \sigma \Leftrightarrow (\exists b \in B; (a,b) \in \rho \wedge (b,c) \in \sigma) \Leftrightarrow (\exists b \in B; (c,b) \in \sigma^{-1} \wedge (b,a) \in \rho^{-1}) \Leftrightarrow (c,a) \in \sigma^{-1} \circ \rho^{-1}$, proto $(\rho \circ \sigma)^{-1} = \sigma^{-1} \circ \tau^{-1}$.

□

## 2.4 Zobrazení množin

V této části se budeme zabývat zobrazeními množin, která budeme chápat jako speciální případ binárních relací mezi množinami.

**Definice 2.10** *Binární relace $f$ mezi množinami $A$ a $B$ se nazývá* zobrazení množiny $A$ do množiny $B$ *(značíme $f : A \longrightarrow B$), platí-li*

*a)* $\forall a \in A \exists b \in B; (a,b) \in f$;

*b)* $\forall a \in A, b_1, b_2 \in B; [(a,b_1) \in f \wedge (a,b_2) \in f] \Rightarrow b_1 = b_2$.

(Množina $A$ se také někdy nazývá *obor* a množina $B$ *koobor* zobrazení $f$.)

`Poznámka:` Podle definice je tedy každému prvku $a \in A$ přiřazen právě jeden prvek z množiny $B$, který se často označuje $f(a)$. Pokud můžeme určit nějaký „předpis“, pomocí kterého jsou vyjádřeny obrazy prvků z $A$, pak označení $f : a \mapsto f(a)$ znamená, že prvku $a$ je přiřazen prvek $f(a) \in B$. Např. podle předpisu $f : x \mapsto 2x$ můžeme určit zobrazení $f : \mathbb{N} \longrightarrow \mathbb{N}$, které každému přirozenému číslu $x$ přiřazuje číslo $2x$.

Označme symbolem $\mathrm{Im} f$ podmnožinu v kooboru $B$ takovou, že $\mathrm{Im} f = \{f(a); a \in A\} = \{b \in B; (\exists a \in A); (a,b) \in f\}$. Množinu $\mathrm{Im} f$ budeme nazývat *obraz množiny $A$ v zobrazení $f$*.

Zavedeme si ještě nejdůležitější typy zobrazení.

**Definice 2.11** *Zobrazení $f : A \longrightarrow B$ se nazývá*

*a)* injektivní *(nebo* prosté*), jestliže platí*

$$\forall a_1, a_2 \in A, b \in B; [(a_1, b) \in f \wedge (a_2, b) \in f] \Rightarrow a_1 = a_2;$$

*b)* surjektivní *(nebo* zobrazení $A$ na $B$*), platí-li*

$$\forall b \in B \exists a \in A; (a,b) \in f \ (\textit{tj. když } \mathrm{Im} f = B);$$

*c)* bijektivní *(nebo* vzájemně jednoznačné zobrazení $A$ na $B$*), je-li současně injektivní i surjektivní.*

**Příklad 2.6**

a) Nechť $A = \{a,b,c\}, B = \{1,2,3\}, \rho = \{(a,2),(a,3),(b,1)\}$. Relace $\rho \subseteq A \times B$ není zobrazením $A$ do $B$. (Dokonce není splněna ani jedna z podmínek z definice 2.10.)

b) Přiřadíme-li libovolnému reálnému číslu $x$ jeho absolutní hodnotu $|x|$, dostaneme zobrazení $g : R \longmapsto R$, které není ani injektivní ani surjektivní.

c) Zobrazení $h : \mathbb{N} \longrightarrow \mathbb{N}$ takové, že $h : n \longmapsto n^2$ je injektivní, není ale surjektivní.

d) Označme $P$ množinu všech trojúhelníků v rovině a $Q$ množinu všech kružnic v téže rovině. Uvažujeme zobrazení $k : C \longrightarrow D$, které každému trojúhelníku přiřazuje kružnici jemu opsanou. Zobrazení $k$ je surjektivní, ale není injektivní.

e) Zobrazení $f : \mathbb{R}^+ \longrightarrow \mathbb{R}$ takové, že $f : x \longmapsto logx$, je bijektivní.

`Poznámka:` Uvědomme si ještě, že podle definice 2.10 se dvě zobrazení $f : A \longrightarrow B$ a $f_1 : A_1 \longrightarrow B_1$ sobě rovnají právě tehdy, platí-li $A = A_1, B = B_1$ a $f(a) = f_1(a)$ pro každý prvek $a \in A$. S měnícím se oborem a kooborem se mohou měnit také vlastnosti zobrazení.

V příkladu 2.6b) je zobrazení $g_1 : \mathbb{R}^+ \longrightarrow \mathbb{R}$, v němž obrazy prvků z $\mathbb{R}^+$ dostaneme stejně jako v $g$, injektivní, ale není surjektivní; zobrazení $g_2 : \mathbb{R} \longrightarrow \mathbb{R}_0^+$ dané předpisem $g_2 : x \longmapsto |x|$, je surjektivní, ale není injektivní.

Protože zobrazení jsou zvláštními typy binárních relací, můžeme je také skládat a vytvářet k nim inverzní relace. Skládáme-li dvě zobrazení, dostaneme ve výsledku opět zobrazení. Přesněji: Jestliže $f : A \longrightarrow B$ a $g : B \longrightarrow C$ jsou zobrazení, pak relace $f \circ g$ je zobrazení množiny $A$ do množiny $C$ a platí $(f \circ g)(x) = g(f(x))$ pro každý $x \in A$. Podle věty 2.6 je skládání binárních relací asociativní, proto je asociativní i skládání zobrazení.

Obecně však inverzní relace $f^{-1}$ k zobrazení $f : A \longrightarrow B$ nemusí být zobrazením. Např. je-li $A = \{a, b\}, B = \{0, 1\}, f = \{(a, 0), (b, 0)\}$, pak inverzní relace $f^{-1} = \{(0, a), (0, b)\} \subseteq B \times A$ není zobrazením $B$ do $A$. Je zřejmé, že aby byla splněna podmínka a) z definice 2.10 i pro relaci $f^{-1}$, musí být zobrazení $f$ surjektivní, a pro platnost podmínky b) z téže definice pro relaci $f^{-1}$ musí být $f$ injektivní. Proto inverzní relace $f^{-1}$ je zobrazením právě tehdy, je-li zobrazení $f$ bijektivní. V takovémto případě je $f^{-1}$ také bijektivním zobrazením ($f^{-1} : B \longrightarrow A$) a nazývá se *inverzním zobrazením* k zobrazení $f$. Označíme-li $id_A = \{(x, x); x \in A\}$, pak pro bijektivní zobrazení $f$ platí $f \circ f^{-1} = id_A$. Podobně $f^{-1} \circ f = id_B$.

Všimněme si ještě blíže některých zobrazení konečných množin.

**Definice 2.12**

a) *Nechť $A$ je konečná neprázdná množina. Potom každé zobrazení $f : A \longrightarrow A$ se nazývá* transformace *množiny $A$.*

b) *Každá bijektivní transformace množiny $A$ se nazývá* permutace *množiny $A$.*

Pro transformace konečných množin budeme s výhodou využívat zápisů ve tvaru dvouřádkových schémat. Je-li $A = \{a_1, \ldots, a_n\}$ množina s $n$ prvky, $f : A \longrightarrow A$ transformace, pak $f$ zapíšeme schematicky

$$f = \begin{pmatrix} a_{i_1} & a_{i_2} & \ldots & a_{i_n} \\ f(a_{i_1}) & f(a_{i_2}) & \ldots & f(a_{i_n}) \end{pmatrix},$$

kde v horním řádku jsou vypsány všechny prvky množiny $A$ (každý prvek právě jednou) a v dolním řádku jsou jejich obrazy v transformaci $f$.

Je vidět, že $f$ bude permutací právě tehdy, jestliže se v dolním řádku vyskytne každý prvek z $A$ (samozřejmě pak také právě jednou). Výhodné je použití takovýchto schémat při skládání transformací a při určování inverzní permutace k dané permutaci.

**Příklad 2.7** Je-li $B = \{1, 2, 3, 4, 5\}$, a jestliže $f_1 : B \longrightarrow B, f_2 : B \longrightarrow B$ jsou transformace takové, že

$$f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 4 & 3 & 1 \end{pmatrix},$$

pak

$$f_1 \circ f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 4 & 3 \end{pmatrix}, f_2 \circ f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 1 & 5 & 2 \end{pmatrix},$$

(Např. $(f_1 \circ f_2)(2) = 4$, protože z tabulek bezprostředně vidíme, že $f_1(2) = 3$ a $f_2(3) = 4$.) Protože $f_1 \circ f_2 \neq f_2 \circ f_1$, vidíme, že skládání transformací není obecně komutativní.

Transformace $f_1$ je permutací, proto k ní existuje inverzní permutace $f_1^{-1}$, kterou dostaneme vzájemnou záměnou obou řádků v daném zápise, tj.

$$f_1 = \begin{pmatrix} 2 & 3 & 5 & 1 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 5 & 3 \end{pmatrix},$$

**Příklad 2.8** Nechť je dána množina $A = \{1, 2\}$. Je zřejmé, že

$$f_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, f_3 = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, f_4 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix},$$

jsou právě transformace množiny $A$. Výsledky skládání těchto transformací zapíšeme přehledně do následující tabulky.

| $\circ$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
|---|---|---|---|---|
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
| $f_2$ | $f_2$ | $f_1$ | $f_3$ | $f_4$ |
| $f_3$ | $f_3$ | $f_4$ | $f_3$ | $f_4$ |
| $f_4$ | $f_4$ | $f_3$ | $f_3$ | $f_4$ |

V této tabulce je výsledek složení $f_i \circ f_j$ transformace $f_i$ s transformací $f_j$ $(i, j = 1, 2, 3, 4)$ umístěn na průsečíku $i$-tého řádku a $j$-tého sloupce.

## 2.5 Cvičení

**2.1**

a) Dokažte všechny nedokázané vlastnosti množinových operací z věty 2.3.

b) Dokažte větu 2.4.

**2.2** Na množině $A = \{1, 2, 3, 4, 5, 6\}$ jsou definovány binární relace $R_1$, $R_2$, $R_3$, $R_4$ postupně výrokovými formami:

$R_1$: $x$ je násobkem $y$;   $R_2$: $x$ není násobkem $y$;
$R_3$: $x$ je dělitelem $y$;   $R_4$: $x$ není dělitelem $y$.

a) Určete výčtem prvků relace $R_1$, $R_2$, $R_3$, $R_4$.

b) Jakým vztahem jsou vázány relace $R_1$, $R_2$ a relace $R_3$, $R_4$?

c) Nakreslete kartézské a uzlové grafy těchto relací.

d) Určete výčtem prvků a charakteristickou vlastností prvků relace $R_1^{-1}$, $R_2^{-1}$, $R_3^{-1}$, $R_4^{-1}$.

[ b) $R_2 = A^2 \setminus R_1$, $R_3 = A^2 \setminus R_4$ ]

**2.3** Označme $A$ množinu všech pravidelných $n$-úhelníků $(n \geq 3)$ a $B$ množinu všech trojúhelníků v rovině. Určete množiny $A \cap B, A \setminus B, B \setminus A$.
[ $A \cap B$ je množina všech rovnostranných trojúhelníků, $A \setminus B$ je množina všech pravidelných n-úhelníků $(n \geq 4)$, $B \setminus A$ je množina všech nerovnostranných trojúhelníků ]

**2.4** Zjistěte, je-li pravdivý výrok

$$\forall A, B, C; (A \setminus B) \cap (A \setminus C) = A \setminus (B \cap C),$$

kde $A, B, C$ jsou množiny.
[ Ne, ukažte protipříklad. ]

**2.5** Určete kolik binárních relací existuje

a) na množině $A$ o $m$ prvcích?

b) mezi prvky množin $A$, $B$, které mají postupně $m$ a $n$ prvků?

[ a) $2^{m^2}$; b) $2^{m \cdot n}$ ]

**2.6** Určete inverzní relaci $\rho^{-1}$ k relaci $\rho \subseteq A \times B$, platí-li

a) $A = \{u, v, w, y, z\}, B = \{\Box, \triangle\}, \rho = \{(x, \triangle), (x, \Box), (u, \Box), (v, \triangle), (z, \Box)\}$;

b) $A = B = N, \forall a, b \in \mathbb{N}(a\rho b \iff a - b = 5c$, kde $c$ je některé celé číslo).

[ a) $\rho^{-1} = \{(\triangle, x), (\Box, x), (\Box, u), (\triangle, v), (\Box, z)\}$; b) $\rho^{-1} = \rho$ ]

**2.7** Nechť $A = \{1, 2, 3\}, B = \{x, y, z\}$, $C = \{\alpha, \beta, \gamma, \delta\}$, $\rho = \{(1, y), (1, z), (2, x), (3, y)\}$, $\sigma = \{(x, ), (y, \alpha), (y, \gamma), (z, \delta)\}$. Určete relaci $\rho \circ \sigma$.
[ $\rho \circ \sigma = \{(1, \alpha), (1, \gamma), (1, \delta), (2, \gamma), (3, \alpha), (3, \gamma)\}$ ]

**2.8** Zapište všechny binární relace na dvouprvkové množině $A = \{1, 2\}$. Určete všechny relace $\delta$ na $A$, pro které platí $\rho \circ \delta = \delta \circ \rho$, kde $\rho = \{(1, 1), (1, 2), (2, 1)\}$.

**2.9** Na množině $A = \{a, b, c, d\}$ jsou dány binární relace $R_1 = \{(a, a), (a, b), (a, c), (b, d)\}$, $R_2 = \{(a, b), (c, d), (c, b)\}$, $R_3 = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, a), (b, c), (c, b)\}$. Určete výčtem prvků relace $R_2 \circ R_1$, $R_1 \circ R_2$, $R_3 \circ R_1$, $R_3 \circ R_3$, $R_1 \circ (R_2 \circ R_3)$, $R_1^{-1}$, $R_2^{-1}$, $R_3^{-1}$, $R_3^{-1} \circ R_2^{-1} \circ R_1^{-1}$.

**2.10** Nechť $R$, $R_1$, $R_2$ jsou relace mezi $A$ a $B$ a $S$, $S_1$, $S_2$ relace mezi $B$ a $C$. Jaké množinové vztahy platí pro:

a) $R \circ (S_1 \cup S_2) \qquad R \circ S_1 \cup R \circ S_2$;

b) $(R_1 \cup R_2) \circ S \qquad R_1 \circ S \cup R_2 \circ S$;

c) $R \circ (S_1 \cap S_2) \qquad R \circ S_1 \cap R \circ S_2$;

d) $(R_1 \cap R_2) \circ S \qquad R_1 \circ S \cap R_2 \circ S$;

e) $R \circ S_1 \setminus R \circ S_2 \qquad R \circ (S_1 \setminus S_2)$;

f) $R_1 \circ S \setminus R_2 \circ S \qquad (R_1 \setminus R_2) \circ S$;

[ a) =; b) =; c) $\subseteq$; d) $\subseteq$; e) $\subseteq$; f) $\subseteq$ ]

**2.11** Dokažte: Pro libovolné relace $\rho, \delta \subseteq A \times B$ platí $\rho \subseteq \delta$ právě tehdy, když $\rho^{-1} \subseteq \delta^{-1}$.

**2.12** Na množině $A = \{a, b, c, d, e, f\}$ jsou dány binární relace
$R_1 = \{(a, d), (c, b), (c, d), (f, f)\}$,
$R_2 = \{(a, f), (b, e), (c, d), (d, c), (e, b), (f, a), (c, f)\}$,
$R_3 = \{(a, b), (b, b), (c, b), (d, e), (e, e), (f, e)\}$,
$R_4 = \{(a, c), (b, a), (c, b), (d, d), (e, f), (f, e)\}$,
$R_5 = \{(a, b), (b, c), (c, d), (d, e), (e, f), (f, a)\}$.

a) Určete, které z relací jsou zobrazení a v těchto případech určete druh zobrazení.

b) Pro každé zobrazení $R_i$, $i \in \{1, \dots, 5\}$ určete obor a koobor.

c) Pro bijekce $R_i$, $i \in \{1, \dots, 5\}$ určete zobrazení inverzní.

d) U každého zobrazení $R_i$, $i \in \{1, \dots, 5\}$ určete úplný vzor a úplný obraz prvku $b$.

e) Jsou-li $R_i$, $R_j$, $i, j \in \{1, \dots, 5\}$ permutace, utvořte složené permutace $R_i \circ R_j$, $R_j \circ R_i$.

[ a)$R_1$, $R_2$ nejsou zobrazení, $R_3$ je zobrazení, $R_4$, $R_5$ jsou bijekce ]

**2.13** Uveďte nutnou a dostatečnou podmínku existence bijekce konečné množiny $A$ na konečnou množinu $B$.
[ stejný počet prvků ]

**2.14** Určete výčtem prvků množiny $S_n$ všech permutací $n$ prvkových množin pro $n \in \{1, 2, 3, 4\}$. V každé množině $S_n$, $n \in \{1, 2, 3\}$ utvořte všechny složené permutace $p_i \circ p_j$ a dále nalezněte inverzní permutace $p_i^{-1}$ pro všechny prvky $S_n$, $n \in \{1, 2, 3, 4\}$.

**2.15** Zjistěte vlastnosti (injektivnost, surjektivnost, bijektivnost) zobrazení $f : \mathbb{R} \longrightarrow \mathbb{R}$ takového, že $\forall x \in \mathbb{R}; f : x \longmapsto ax + b$, kde $a, b \in R$.
[ Je-li $a \neq 0$, pak je $f$ bijektivní; je-li $a = 0$, pak $f$ není ani injektivní ani surjektivní. ]

**2.16** Nechť $T$ je množina všech trojúhelníků v rovině a nechť pro každý $t \in T$ označuje $|t|$ obsah trojúhelníka $t$. Určete vlastnosti zobrazení $g : T \longrightarrow \mathbb{R}$ takového, že $g : t \longmapsto |t|$ ($g_1 : T \longrightarrow \mathbb{R}^+$ takového, že $g_1 : t \longmapsto |t|$).
[ $g$ není ani injektivní ani surjektivní; $g_1$ je surjektivní, není injektivní. ]

**2.17** Dokažte, že zobrazení $\varphi : \mathbb{Z} \longrightarrow 3\mathbb{Z}$ takové, že $\forall x \in \mathbb{Z}; \varphi : x \longmapsto 3x$, je bijektivní. Určete inverzní zobrazení $\varphi^{-1}$. ($3\mathbb{Z} = \{3y; y \in \mathbb{Z}\}$).
[ $\varphi^{-1} : 3\mathbb{Z} \longrightarrow \mathbb{Z}, \varphi^{-1} : y \longmapsto \frac{y}{3}$ ]

**2.18** Napište tabulku pro skládání permutací na tříprvkové množině $A = \{1, 2, 3\}$. Zjistěte z tabulky , zdali je skládání permutací na $A$ komutativní.
[ Existuje 6 permutací a jejich skládání není obecně komutativní. ]

# Kapitola 3

# Algebraické struktury

S algebraickými strukturami se setkáváme od 1. třídy základní školy (i když se explicitně o tomto pojmu nehovoří) při zavádění aritmetických číselných operací. Důkladné studium algebraických struktur bude obsahem přednášek v dalších semestrech. Zde budeme jenom definovat základní pojmy, které budou potřebné pro naše účely, a budeme je ilustrovat zejména na číselných strukturách.

## 3.1 Algebraické struktury s jednou binární operací

**Definice 3.1** *Je-li $G$ neprázdná množina, potom* binární operací *na $G$ rozumíme libovolné zobrazení $\circ : G \times G \to G$.*

Tedy binární operace „$\circ$“ přiřazuje každé uspořádané dvojici $(x, y)$ prvků z $G$ jednoznačně určený prvek $\circ(x, y)$, který budeme značit $x \circ y$ a nazývat *výsledek operace* „$\circ$“ provedené na prvky $x$ a $y$ (v tomto pořadí).

`Poznámka:`

a) Budeme-li hovořit o konkrétních binárních operacích, budeme často místo symbolu „$\circ$“ používat také symboly „$+$“, „$\cdot$“, „$\square$“, apod.

b) Pro libovolné číslo $n \in \mathbb{Z}$, $n \geq 0$, můžeme zavést pojem *$n$-ární operace* na $G$ jako zobrazení kartézské mocniny $G^n$ do množiny $G$. Speciálně pro $n = 2$ dostáváme již zavedený pojem binární operace.

c) Pokud nebude řečeno něco jiného, bude v tomto textu pod názvem „operace“ rozuměna binární operace.

**Příklad 3.1**

a) Sčítání je operací na množině $\mathbb{N}$, zatímco odčítání na $\mathbb{N}$ operací není. (Např. $3+5 \in \mathbb{N}$, ale $3 - 5 \notin \mathbb{N}$.)

b) Odčítání je operací na $\mathbb{Z}$, dělení na $\mathbb{Z}$ není operací.

c) Dělení na $\mathbb{Q}$ není operací (nemůžeme dělit nulou), ale dělení na $\mathbb{Q} \setminus \{0\}$ je operací.

**Definice 3.2** Algebraickou strukturou *$\mathcal{G}$ rozumíme některou neprázdnou množinu $G$ spolu s neprázdným systémem $\{f_\alpha; \alpha \in I\}$ $n$-árních algebraických operací na množině $G$. (Číslo $n$ může být pro různé operace různé.) Značíme $\mathcal{G} = (G, f_\alpha; \alpha \in I)$.*

**Definice 3.3**

a) *Je-li „$\circ$“ binární operace na množině $G \neq \emptyset$, potom algebraická struktura $\mathcal{G} = (G, \circ)$ se nazývá* grupoid.

b) *Je-li operace „$\circ$“ komutativní, tj. platí-li*

$$\forall a, b \in G; a \circ b = b \circ a,$$

*pak se $\mathcal{G}$ nazývá* komutativní grupoid.

**Definice 3.4** Pologrupou *rozumíme libovolný grupoid $\mathcal{G} = (G, \circ)$, ve kterém je operace „$\circ$“ asociativní, tj. platí-li*

$$\forall a, b, c \in G; a \circ (b \circ c) = (a \circ b) \circ c.$$

*Komutativní pologrupu budeme také nazývat* abelovskou.

**Příklad 3.2**

a) Grupoidy $\mathcal{N} = (\mathbb{N}, +)$, $\mathcal{N}' = (\mathbb{N}, \cdot)$, $\mathcal{Z} = (\mathbb{Z}, +)$, $\mathcal{Z} = (\mathbb{Z}, \cdot)$ jsou abelovskými pologrupami.

b) Pologrupami nejsou grupoidy $\mathcal{Z}'' = (\mathbb{Z}, -)$, $\mathcal{Q}_0' = (\mathbb{Q} \setminus \{0\}, :)$, $\mathcal{N}'' = (\mathbb{N}, \Box)$ (kde $a \Box b = a^b$).
Žádný z těchto grupoidů není ani komutativní.

c) Nechť $A$ je konečná neprázdná množina. Označíme-li $T(A)$ množinu všech transformací množiny $A$ a je-li „$\circ$“ operace skládání transformací, potom $\mathcal{T}(A) = (T(A), \circ)$ je pologrupa.

V příkladu 2.8 jsme pro $A = \{1, 2\}$ zapsali výsledky operací v pologrupě $\mathcal{T}(A)$ přehledně do čtvercové tabulky. Podobných tabulek můžeme použít pro libovolné konečné grupoidy. Jsou to čtvercové tabulky, jejichž řádky a sloupce jsou označeny pomocí prvků daného grupoidu (nejlépe v témže pořadí) a na průsečíku řádku označeného prvkem $a$ a sloupce označeného prvkem $b$ leží výsledek operace provedené na prvky $a$ a $b$ (v tomto pořadí). Každou takovou tabulku nazveme *Cayleyova tabulka* daného grupoidu.

**Příklad 3.3** Nechť $\mathbb{Z}_3 = \{0, 1, 2\}$. Označme „$\oplus$“ operaci na $\mathbb{Z}_3$ takovou, že

$$\forall a, b \in \mathbb{Z}_3; a \oplus b = \begin{cases} a + b, & \text{pokud } a + b < 3; \\ (a + b) - 3, & \text{pokud } a + b \geq 3. \end{cases}$$

Následující tabulka je Cayleyovou tabulkou grupoidu $\mathbb{Z}_3 = (Z_3, \oplus)$.

| $\oplus$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

**Definice 3.5** *Řekneme, že grupoid $\mathcal{G} = (G, \circ)$ má* neutrální prvek, *je-li pravdivý výrok*

$$\exists n \in G \forall a \in G; a \circ n = a = n \circ a.$$

*Každý takový prvek $n$ nazýváme* neutrálním prvkem *grupoidu $\mathcal{G}$.*

**Věta 3.1** *V grupoidu $\mathcal{G} = (G, \circ)$ může existovat nejvýše jeden neutrální prvek.*

D ů k a z: Předpokládejme, že v $\mathcal{G}$ existují dva neutrální prvky $n_1$ a $n_2$. Pak podle definice 3.4 platí $n_1 \circ n_2 = n_2$ a současně $n_1 \circ n_2 = n_1$, tedy z jednoznačnosti operace v grupoidu dostáváme $n_1 = n_2$. □

**Definice 3.6** *Nechť grupoid $\mathcal{G} = (G, \circ)$ má neutrální prvek $n$ a nechť $a \in G$. Pak $a^* \in G$ se nazývá* symetrickým prvkem k prvku *$a$, platí-li*

$$a \circ a^* = n = a^* a.$$

**Věta 3.2** *Ke každému prvku pologrupy $\mathcal{G} = (G, \circ)$ s neutrálním prvkem $n$ může existovat nejvýše jeden symetrický prvek.*

D ů k a z: Předpokládejme, že $a$ je prvek pologrupy $\mathcal{G}$ a že $a^*$, $a^+$ jsou symetrické prvky k $a$. Platí tedy $a \circ a^* = a^* \circ a = n$, $a \circ a^+ = a^+ \circ a = n$. Můžeme proto psát

$$a^* = a^* \circ n = a^* \circ (a \circ a^+) = (a^* \circ a) \circ a^+ = n \circ a^+ = a^+,$$

tzn. $a^* = a^+$. □

**Definice 3.7** *Pologrupa $\mathcal{G} = (G, \circ)$ se nazývá* grupa, *obsahuje-li neutrální prvek a existuje-li v ní ke každému prvku symetrický prvek, tj. jsou-li pravdivé výroky*

$$\exists n \in G \forall a \in G; a \circ n = a = n \circ a,$$

$$\forall a \in G \exists a^* \in G; a \circ a^* = n = a^* \circ a.$$

*Komutativní grupa se také nazývá* abelovská.

`Poznámka`: Pro binární operace budeme nejčastěji používat označení „$\cdot$“ a „$+$“. Pokud použijeme operaci „$\cdot$“, řekneme, že grupoid $\mathcal{G} = (G, \cdot)$ je *multiplikativní*. Výsledek operace $a \cdot b$ budeme nazývat *součin* prvků $a$ a $b$ a budeme jej také zapisovat $ab$. Pokud existuje neutrální prvek, označíme jej $e$ a budeme nazývat *jednotkový prvek*. Pokud k prvku $a$ pologrupy $G$ existuje symetrický prvek, označíme jej $a^{-1}$ a nazveme *inverzní prvek* k $a$.

Grupoid $\mathcal{G} = (G, +)$ nazýváme *aditivní*, výsledek operace $a+b$ nazveme *součet* prvků $a$ a $b$, neutrální prvek označíme „$o$“ a nazveme *nulový prvek* a symetrický prvek k $a$ označíme $-a$ a nazveme *opačný prvek* k $a$.

**Příklad 3.4**

a) V pologrupě $\mathcal{N} = (N, +)$ neexistuje nulový prvek. V $\mathcal{Z} = (\mathbb{Z}, +)$ je nulovým prvkem číslo 0, opačným prvkem k číslu $a$ je číslo $-a$, tedy $\mathcal{Z}$ je komutativní grupa.

b) V pologrupě $\mathcal{N}' = (\mathbb{N}, \cdot)$ je jednotkovým prvkem číslo 1, inverzní prvek existuje pouze k číslu 1 ($1^{-1} = 1$). V pologrupě $\mathcal{Z}' = (\mathbb{Z}, \cdot)$ je jednotkovým prvkem také číslo 1, inverzní prvky existují jenom k číslům 1 a $-1$

c) $\mathcal{Q} = (\mathbb{Q}, +)$, $\mathcal{R} = (\mathbb{R}, +)$, $\mathcal{C} = (\mathbb{C}, +)$ jsou aditivní komutativní grupy. V pologrupě $\mathcal{Q}' = (\mathbb{Q}, \cdot)$ je jednotkovým prvkem číslo 1, inverzním prvkem k číslu $a \neq 0$ je inverzní číslo $a^{-1}$, ale k číslu 0 inverzní prvek neexistuje, proto $\mathcal{Q}'$ není grupa. Podobně nejsou grupami pologrupy $\mathcal{R}' = (\mathbb{R}, \cdot)$ a $\mathcal{C}' = (\mathbb{C}, \cdot)$.
Pokud ale uvažujeme místo množin $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ množiny $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$, pak $\mathcal{Q}_0 = (\mathbb{Q} \setminus \{0\}, \cdot)$, $\mathcal{R}_0 = (\mathbb{R} \setminus \{0\}, \cdot)$, $\mathcal{C}_0 = (\mathbb{C} \setminus \{0\}, \cdot)$ jsou multiplikativní komutativní grupy.

d) Nechť $A$ je konečná neprázdná množina, $T(A)$ množina všech transformací a $S(A)$ množina všech permutací množiny $A$. Potom každá z pologrup $\mathcal{T}(A) = (T(A), \circ)$ a $\mathcal{S}(A) = (S(A), \circ)$ má jednotkový prvek, kterým je identita na $A$. Přitom $\mathcal{S}(A)$ je grupou, protože inverzním prvkem k permutaci $f$ je inverzní permutace $f^{-1}$. Pokud má množina $A$ alespoň tři prvky, pak $\mathcal{S}(A)$ není komutativní.

## 3.2 Algebraické struktury se dvěma binárními operacemi

V této části budeme definovat základní typy algebraických struktur se dvěma binárními operacemi. K jejich popisu budeme s výhodou využívat právě zavedených pojmů.

**Definice 3.8** Okruhem *nazýváme algebraickou strukturu* $\mathcal{M} = (M, +, \cdot)$ *se dvěma binárními operacemi „$+$“ a „$\cdot$“ takovou, že* $(M, +)$ *je komutativní grupa,* $(M, \cdot)$ *je pologrupa a operace násobení je zleva i zprava distributivní vzhledem k operaci sčítání, tj. platí-li*

**A1** $\forall a, b \in M; a + b = b + a,$

**A2** $\forall a, b, c \in M; a + (b + c) = (a + b) + c,$

**A3** $\exists o \in M \forall a \in M; a + o = a,$

**A4** $\forall a \in M \exists -a \in M; a + (-a) = o,$

**M1** $\forall a, b, c \in M; a(bc) = (ab)c,$

$\mathbf{D}_L$ $\forall a, b, c \in M; a(b + c) = ab + ac,$

$\mathbf{D}_P$ $\forall a, b, c \in M; (a + b)c = ac + bc.$

*Je-li pologrupa $(M, \cdot)$ komutativní, tj. platí-li*

**M2** $\forall a, b \in M; ab = ba,$

*pak se okruh $\mathcal{M}$ nazývá* komutativní.

`Poznámka`: Jsou-li $a, b \in M$, pak místo $a + (-b)$ budeme psát také krátce $a - b$. Protože pro libovolné $a, b, c \in M$ vždy platí $ab = a[c+(b-c)] = ac+a(b-c)$, a tedy $a(b-c) = ab-ac$, je násobení také distributivní zleva vzhledem k odčítání.

Analogicky $ba = [c + (b - c)]a = ca + (b - c)a$, tzn. $(b - c)a = ba - ca$, proto je násobení distributivní vzhledem k odčítání i zprava.

Dále je-li $a \in M$, pak

$$a(a - a) = aa - aa = o, (a - a)a = aa - aa = o,$$

tedy $ao = o = oa$.

**Příklad 3.5**

a) Víme, že $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ jsou komutativní grupy a že $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ jsou komutativní pologrupy. Protože násobení čísel je distributivní vzhledem ke sčítání, jsou $\mathcal{Z} = (\mathbb{Z}, +, \cdot)$, $\mathcal{Q} = (\mathbb{Q}, +, \cdot)$, $\mathcal{R} = (\mathbb{R}, +, \cdot)$ a $\mathcal{C} = (\mathbb{C}, +, \cdot)$ komutativní okruhy.

b) $\mathcal{O} = (\{0\}, +, \cdot)$ je také komutativní okruh.

c) Algebraická struktura $\mathcal{N} = (\mathbb{N}, +, \cdot)$ není okruhem, protože $(\mathbb{N}, +)$ není grupa.

**Příklad 3.6** Nechť $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Uvažujme na $\mathbb{Z}_4$ binární operace „$\oplus$“ a „$\otimes$“ zadané následujícími Cayleyovými tabulkami:

| $\oplus$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

| $\otimes$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

Můžeme snadno ověřit, že obě tyto operace jsou asociativní a komutativní a že násobení „$\otimes$“ je distributivní vzhledem ke sčítání „$\oplus$“. Přitom nulovým prvkem v $(\mathbb{Z}, \oplus)$ je číslo 0 a platí $-0 = 0$, $-1 = 3$, $-2 = 2$, $-3 = 1$, tedy ke každému prvku existuje prvek opačný. Proto $\mathcal{Z}_4 = (\mathbb{Z}_4, \oplus, \otimes)$ je komutativní okruh.

**Definice 3.9** Číselným okruhem *rozumíme každý takový okruh $\mathcal{M} = (M, +, \cdot)$, že $M$ je podmnožinou množiny všech komplexních čísel $\mathbb{C}$ a pro libovolné prvky $a, b \in M$ je součet $a + b$, resp. součin $ab$, roven obyčejnému součtu, resp. součinu, komplexních čísel $a, b$.*

`Poznámka:`

a) Okruhy $\mathcal{Z}$, $\mathcal{Q}$, $\mathcal{R}$, $\mathcal{C}$ a $\mathcal{O}$ z příkladu 3.5 jsou číselnými okruhy, zatímco okruh $\mathcal{Z}_4$ není číselným okruhem, i když platí $\mathbb{Z}_4 \subseteq \mathbb{C}$. (Později budeme pracovat i s jinými typy okruhů, které nebudou číselné.)

b) Násobení i sčítání komplexních čísel jsou komutativní a asociativní operace a násobení je distributivní vzhledem ke sčítání. Proto pro libovolnou neprázdnou podmnožinu $A$ množiny $\mathbb{C}$ platí, že $A$ je číselným okruhem (spolu s číselným sčítáním a násobením), jestliže

1. $\forall a, b \in A; a + b \in A$,
2. $0 \in A$,
3. $\forall a \in A; -a \in A$,
4. $\forall a, b \in A; ab \in A$.

**Definice 3.10**

a) *Prvek $a \neq o$ okruhu $\mathcal{M} = (M, +, \cdot)$ se nazývá* levý *(*pravý*)* netriviální dělitel nuly, *existuje-li nenulový prvek $b \in M$ takový, že $ab = o$ $(ba = o)$.*

b) *Řekneme, že $a \neq o$ je* netriviálním dělitelem nuly, *je-li $a$ současně levým i pravým netriviálním dělitelem nuly.*

**Definice 3.11** Oborem integrity *budeme rozumět každý okruh $\mathcal{J} = (J, +, \cdot)$, který je komutativní, obsahuje jednotkový prvek (vzhledem k násobení) $e \neq o$ a ve kterém neexistují netriviální dělitelé nuly.*

*Tj. kromě vlastností komutativního okruhu z definice 3.8 platí*

**M3** $\exists o \neq e \in J \forall a \in J; ae = a,$

**M4** $\forall a, b \in J; (ab = o \wedge a \neq o) \Rightarrow b = o.$

**Příklad 3.7**

a) Vzhledem k tomu, že každý číselný okruh je komutativní a že pro násobení komplexních čísel neexistují netriviální dělitelé nuly, bude číselný okruh $\mathcal{M} = (M, +, \cdot)$ oborem integrity právě tehdy, bude-li $1 \in M$. Tedy $\mathcal{Z}$, $\mathcal{Q}$, $\mathcal{R}$, $\mathcal{C}$ jsou *číselnými obory integrity*, zatímco $\mathcal{O}$ není číselným oborem integrity. Podobně, označíme-li $2\mathbb{Z}$ množinu všech sudých celých čísel, pak $2\mathcal{Z} = (2\mathbb{Z}, +, \cdot)$ je číselným okruhem, který ale není oborem integrity.

b) Okruh $\mathcal{Z}_4$ z příkladu 3.6 je komutativní, číslo 1 je jednotkovým prvkem v $\mathcal{Z}_4$ a platí $1 \neq 0$. Přitom $\mathcal{Z}_4$ není oborem integrity, protože platí $0 \neq 2$, ale $2 \otimes 2 = 0$, tedy $\mathcal{Z}_4$ obsahuje netriviální dělitel nuly.

**Definice 3.12**

a) *Okruh $\mathcal{T} = (T, +, .)$ se nazývá* těleso, *jestliže $T$ obsahuje alespoň dva navzájem různé prvky a je-li $(T \setminus \{0\}, \cdot)$ grupou.*
*Jinými slovy, pro okruh $\mathcal{T}$ obsahující alespoň dva různé prvky jsou splněny podmínky*

$\mathbf{M}_3'$ $\exists o \neq e \in T \forall o \neq a \in T; ae = a = ea,$

$\mathbf{M}_4'$ $\forall o \neq a \in T \exists o \neq a^{-1} \in T; aa^{-1} = e = a^{-1}a.$

b) *Je-li $(T, \cdot)$ komutativní, pak se $\mathcal{T}$ nazývá* komutativní těleso.

**Věta 3.3**

a) *Těleso nemůže obsahovat netriviální dělitele nuly.*

b) *Každé komutativní těleso je oborem integrity.*

D ů k a z:

a) Nechť $\mathcal{T} = (T, +, \cdot)$ je těleso. Předpokládejme, že $a \in T$ je levým netriviálním dělitelem nuly. Tzn., že existuje $o \neq b \in T$ takový, že $ab = o$. Protože $a$ je nenulový prvek, existuje k němu v $T$ inverzní prvek $a^{-1}$. Z rovnosti $ab = o$ proto dostáváme rovnost $a^{-1}(ab) = a^{-1}o$ tj. $(a^{-1}a)b = o$, a odtud $b = o$. Prvek $b$ je ale podle předpokladu nenulový, to je spor.

b) Předpokládejme, že $\mathcal{T} = (T, +, \cdot)$ je komutativní těleso. Podle části a) $\mathcal{T}$ neobsahuje netriviální dělitele nuly. Proto stačí dokázat, že pologrupa $(T, \cdot)$ má jednotkový prvek. Z definice tělesa vyplývá, že existuje jednotkový prvek $e$ v $(T \setminus \{0\}, +, \cdot)$. Ovšem platí také $oe = o$, a proto je $e$ jednotkovým prvkem celé pologrupy $(T, \cdot)$.

$\square$

**Příklad 3.8**

a) Číselný okruh, který je tělesem, budeme nazývat *číselné těleso*. Protože každé číselné těleso je komutativní, je podle věty 3.3 také číselným oborem integrity. Víme, že $(\mathbb{Z} \setminus \{0\}, \cdot)$ není grupa, proto $\mathcal{Z} = (\mathbb{Z}, +, \cdot)$ není číselným tělesem. Každá z pologrup $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$ je grupou, tedy $\mathcal{Q} = (\mathbb{Q}, +, \cdot)$, $\mathcal{R} = (\mathbb{R}, +, \cdot)$, $\mathcal{C} = (\mathbb{C}, +, \cdot)$ jsou číselná tělesa.

b) Komutativní okruh $\mathcal{Z}_4 = (\mathbb{Z}_4, \oplus, \otimes)$ není oborem integrity, proto nemůže být podle věty 3.3 ani tělesem.

c) V příkladu 3.3 jsme uvažovali aditivní operaci „$\oplus$“ na množině $\mathbb{Z}_3 = \{0, 1, 2\}$. Definujme nyní, analogicky jako pro $\mathcal{Z}_4$, také multiplikativní operaci „$\otimes$“. Obě operace jsou dány následujícími Cayleyovými tabulkami:

| $\oplus$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

| $\otimes$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

Je vidět, že $(\mathbb{Z}_3, \oplus)$ je komutativní grupa (nulovým prvkem je 0 a platí $-0 = 0$, $-1 = 2$, $-2 = 1$) a že $(\mathbb{Z}_3 \setminus \{0\}, \otimes)$ je také komutativní grupa (jednotkovým prvkem je 1, $1^{-1} = 1$, $2^{-1} = 2$). Platí, že $\mathcal{Z}_3 = (\mathbb{Z}_3, \oplus, \otimes)$ je komutativní těleso. (Platnost zbývajících podmínek si může čtenář ověřit sám.)

## 3.3 Cvičení

**3.1** Zjistěte, je-li

a) sčítání na $\mathbb{Z}_0$,

b) sčítání na $\mathbb{Z}^-$,

c) sčítání na $\{-1, 1\}$,

d) sčítání na $\mathbb{R} \setminus \mathbb{Q}$ (tj. na množině všech iracionálních čísel),

e) násobení na $\mathbb{C}_0$,

f) násobení na $\mathbb{Z}^-$,

g) násobení na $\mathbb{R} \setminus \mathbb{Q}$,

h) násobení na $\{-1, 1\}$,

i) dělení na $\mathbb{Q}_0$,

j) odčítání na $\mathbb{C}$,

k) umocňování na $\mathbb{Z}$

binární operací na příslušné množině.
[ a),c),d),f),g),k) není; b),e),h),i),j) je ]

**3.2** Nechť pro libovolná $a, b \in \mathbb{N}$ označuje $a\Box b$ prvek $a^b$. Určete všechny takové trojice $(a, b, c) \in N^3$, pro které platí

$$a\Box(b\Box c) = (a\Box b)\Box c.$$

[ $(1, x, y)$, $(x, y, 1)$, $(x, 2, 2)$ kde $x, y$ jsou libovolná čísla z $\mathbb{N}$. ]

**3.3** Nechť pro libovolná reálná čísla $a, b$ platí

$$a\Box b = a + b + 1, a\triangle b = a + b + ab.$$

Dokažte, že

a) $(\mathbb{R}, \Box)$ je abelovská grupa;

b) $(\mathbb{R}, \triangle)$ je abelovská pologrupa s neutrálním prvkem, která ale není grupou.

**3.4** Nechť je dána rovina $\rho$. Označme pro libovolné body $A, B \in \rho$ symbolem $A * B$ střed úsečky $AB$. Určete vlastnosti grupoidu $(\rho, *)$.
[ Komutativní grupoid, není pologrupou, neexistuje neutrální prvek. ]

**3.5** Jakou podmínku musí splňovat množina $A$, aby grupoid $(\mathcal{P}(A), \cap)$ byl grupou? (Zde $\mathcal{P}(A)$ označuje množinu $\{X; X \subseteq A\}$.)
[ $A = \emptyset$ ]

**3.6** Zjistěte, je-li následující uspořádaná trojice okruhem. Pokud se jedná o okruh, zjistěte jeho vlastnosti (komutativnost, existenci jednotkového prvku, existenci dělitelů nuly, je-li oborem integrity, popř. tělesem):

a) $(2\mathbb{Z}+1, +, \cdot)$ ($2\mathbb{Z}+1$ ... množina všech celých lichých čísel),

b) $(\mathbb{Q}_0, +, \cdot)$,

c) $(3\mathbb{Z}, +, \cdot)$,

d) $(\mathbb{R} \setminus \mathbb{Q}, +, \cdot)$,

e) $(\{1, -1\}, +, \cdot)$,

f) $(\mathbb{R}, \square, \triangle)$ ($\square$ a $\triangle$ mají stejný význam jako v příkladu 3.7).

[ a),b),d),e) není okruh; c) komutativní okruh, nemá jednotkový prvek, neobsahuje netriviální dělitele nuly.; f) komutativní těleso ]

**3.7** Dokažte, že $\mathcal{Z}$ je nejmenším číselným oborem integrity. (Tzn., že je-li $\mathcal{J}$ číselným obor integrity, potom $\mathcal{Z} \subseteq \mathcal{J}$.)

**3.8** Dokažte, že $\mathcal{Q}$ je nejmenším číselným tělesem.

**3.9** Nechť $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Z}\}$. Dokažte, že $\mathcal{Z}[\sqrt{2}] = (\mathbb{Z}[\sqrt{2}], +, \cdot)$ je číselný obor integrity a že je to nejmenší číselný obor integrity, který obsahuje číslo $\sqrt{2}$.

**3.10** Nechť $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3}; a, b \in \mathbb{Q}\}$. Dokažte, že $\mathcal{Q}(\sqrt{3}) = (\mathbb{Q}(\sqrt{3}), +, \cdot)$ je nejmenší číselné těleso, které obsahuje $\sqrt{3}$.

**3.11** Zjistěte, je-li okruh $\mathcal{Z}_6 = (\mathbb{Z}_6, \oplus, \otimes)$, kde $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ a operace „$\oplus$“ a „$\otimes$“ jsou dány tabulkami

| $\oplus$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

| $\otimes$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

integrity, popř. tělesem.
[ není obor integrity ]

# Kapitola 4

# Matice

V této části zavedeme pojem matice nad číselným tělesem, který je významným prostředkem při vyjadřování úvah týkajících se lineární algebry. Zejména se nyní budeme věnovat vlastnostem operací prováděných s maticemi.

## 4.1 Operace s maticemi

**Definice 4.1** *Nechť* $\mathcal{T} = (T, +, \cdot)$ *je číselné těleso,* $m, n \in \mathbb{N}$, $a_{ij} \in T$, $i = 1, \ldots, m$, $j = 1, \ldots, n$. *Potom schéma*

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}, \text{ popř } A = \left\| \begin{matrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{matrix} \right\|,$$

*se nazývá* matice typu $m \times n$ nad $\mathcal{T}$.

*Je-li* $a_{ij}$ *prvek matice, pak číslo* $i$ *nazveme* řádkový index *a číslo* $j$ sloupcový index *tohoto prvku.*

*Je-li* $r = \min\{m, n\}$, *pak řekneme, že prvky* $a_{11}$, $a_{22}$, …, $a_{rr}$ *tvoří* hlavní diagonálu *a prvky* $a_{1n}$, $a_{2,n-1}$, …, $a_{r,n-(r-1)}$ *tvoří* vedlejší diagonálu *matice* $A$.

`Poznámka`: Matici $A$ typu $m \times n$ můžeme také někdy zapisovat ve zkráceném tvaru

$$A = ||a_{ij}||_{m \times n} = ||a_{ij}||_{m,n} = (a_{ij})_{m \times n} = (a_{ij})_{m,n}$$

nebo, pokud bude znám typ matice, také ve tvaru

$$A = ||a_{ij}|| = (a_{ij}).$$

**Příklad 4.1** Matice

$$A = \begin{pmatrix} 2 & -\frac{3}{2} & \frac{4}{3} \\ -5 & 0 & \frac{1}{4} \end{pmatrix}$$

je typu $2 \times 3$ nad $\mathbb{Q}$ (popř. nad $\mathbb{R}$, $\mathbb{C}$), matice

$$A = \begin{pmatrix} \frac{\pi}{2} & \sqrt{3} \\ 2 & 2\pi \end{pmatrix}$$

je typu $2 \times 2$ nad $\mathbb{R}$ (popř. nad $\mathbb{C}$).

**Definice 4.2** *Matice $N_{m\times n} = ||n_{ij}||_{m\times n}$ se nazývá* nulová matice *typu $m \times n$, platí-li $n_{ij} = 0$ pro každé $i = 1, \ldots, m$, $j = 1, \ldots, n$. Bude-li zřejmý typ matice, budeme psát místo $N_{m\times n}$ pouze $N$.*

**Definice 4.3**

a) *Matici $A = ||a_{ij}||$ typu $n \times n$ nazveme* čtvercová matice stupně $n$.

b) *Čtvercovou matici nazveme* diagonální, *pokud všechny její prvky, které neleží na hlavní diagonále, jsou rovny 0.*

c) *Diagonální matice se nazývá* skalární, *jestliže všechny její prvky ležící na hlavní diagonále jsou si rovny.*

d) *Skalární matice, jejíž všechny prvky na hlavní diagonále jsou rovny 1, se nazývá* jednotková matice stupně $n$. *Označíme ji $E_n$ (popř. pokud je zřejmý typ matic, jenom $E$).*

**Příklad 4.2** Budeme uvažovat matice nad $\mathbb{Q}$. Označme

$$A = \begin{pmatrix} 2 & 1 \\ 0 & -3 \end{pmatrix}, B = \begin{pmatrix} 5 & 0 \\ 0 & 0 \end{pmatrix}, C = \begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix}, E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Platí, že $A$ je čtvercová matice stupně 2, která není diagonální, $B$ je diagonální, ale není skalární, $C$ je skalární a $E$ je jednotková matice stupně 2.

`Označení:` Dohodněme se, že 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 $M_n(\mathcal{T})$.

V lineární algebře, kde budeme matice velmi často používat, se nepracuje jenom s jednotlivými maticemi, ale je nutno vytvářet z daných matic další matice. Definice a základní vlastnosti operací s maticemi budou obsahem našich dalších úvah.

**Definice 4.4** *Jsou-li $A = ||a_{ij}||$, $B = ||b_{ij}||$ dvě matice z $M_{m\times n}(\mathcal{T})$, pak řekneme, že matice $A$* je rovna matici $B$, *platí-li $a_{ij} = b_{ij}$ pro každé $i = 1, \ldots, m$, $j = 1, \ldots, n$. Značíme $A = B$.*

**Věta 4.1** *Jsou-li $A, B, C \in M_{m\times n}(\mathcal{T})$, pak platí*

*1)* $A = A$,

*2)* $A = B \Rightarrow B = A$,

*3)* $(A = B \wedge B = C) \Rightarrow A = C$,

*tzn., že rovnost matic z množiny* $M_{m\times n}(\mathcal{T})$ *je reflexivní, symetrická a tranzitivní.*

D ů k a z: Je zřejmý. □

**Definice 4.5** *Nechť* $A = ||a_{ij}||$, $B = ||b_{ij}|| \in M_{m\times n}(\mathcal{T})$. *Potom* součtem *matic* $A$ *a* $B$ *rozumíme matici* $A + B = ||c_{ij}|| \in M_{m\times n}(\mathcal{T})$ *takovou, že* $c_{ij} = a_{ij} + b_{ij}$ *pro každé* $i = 1, \ldots, m$, $j = 1, \ldots, n$.

**Příklad 4.3** Nechť

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

Potom

$$A + B = \begin{pmatrix} 1 & 3 & 3 \\ -4 & 9 & -6 \end{pmatrix}.$$

**Věta 4.2** *Množina* $M_{m\times n}(\mathcal{T})$ *spolu s operací sčítání matic je komutativní grupa.*

D ů k a z: Jsou-li $A, B \in M_{m\times n}(\mathcal{T})$, potom jejich součet $A + B$ patří podle definice 4.5 také do $M_{m\times n}(\mathcal{T})$, takže sčítání matic je binární operací na této množině. Tzn., že $(M_{m\times n}(\mathcal{T}), +)$ je grupoid. Nyní máme ukázat, že grupoid $(M_{m\times n}(\mathcal{T}), +)$ je asociativní a komutativní, obsahuje nulový prvek a s každým prvkem také prvek k němu opačný. Nechť tedy $A = ||a_{ij}||, B = ||b_{ij}||, C = ||c_{ij}|| \in M_{m\times n}(\mathcal{T})$.

Pak

$$(||a_{ij}|| + ||b_{ij}||) + ||c_{ij}|| = ||a_{ij} + b_{ij}|| + ||c_{ij}|| = ||(a_{ij} + b_{ij}) + c_{ij}||.$$

Protože sčítání v tělese $\mathcal{T}$ je asociativní, platí

$$(a_{ij} + b_{ij}) + c_{ij} = a_{ij} + (b_{ij} + c_{ij}),$$

tedy

$$||(a_{ij} + b_{ij}) + c_{ij}|| = ||a_{ij} + (b_{ij} + c_{ij})|| =$$
$$= ||a_{ij}|| + ||b_{ij} + c_{ij}|| = ||a_{ij}|| + (||b_{ij}|| + ||c_{ij}||).$$

Proto platí $(A + B) + C = A + (B + C)$.

Podobně dostaneme (využijeme-li komutativnost sčítání v tělese $\mathcal{T}$)

$$A + B = ||a_{ij}|| + ||b_{ij}|| = ||a_{ij} + b_{ij}|| = ||b_{ij} + a_{ij}|| = ||b_{ij}|| + ||a_{ij}|| = B + A.$$

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

$$A + N = ||a_{ij}|| + ||0|| = ||a_{ij} + 0|| = ||a_{ij}|| = A,$$

tedy $N$ je nulovým prvkem v $(M_{m\times n}(\mathcal{T}),+)$.

Označíme-li $-A = ||-a_{ij}||$, pak platí

$$A + (-A) = ||a_{ij}|| + ||-a_{ij}|| = ||a_{ij} + (-a_{ij})|| = ||0|| = N,$$

proto $-A$ je opačným prvkem v $(M_{m\times n}(\mathcal{T}),+)$ k matici $A$. (Matici $-A$ budeme nazývat *opačná matice k matici* $A$.) $\square$

Sčítání matic stejného typu je příkladem binární operace na množině $M_{m\times n}(\mathcal{T})$, protože libovolnou dvojici matic z $M_{m\times n}(\mathcal{T})$ je určena jednoznačně další matice z této množiny. Nyní si ukážeme, že můžeme přiřadit jednoznačně matici z $M_{m\times n}(\mathcal{T})$ libovolnému prvku z $\mathcal{T}$ a libovolné matici z $M_{m\times n}(\mathcal{T})$. Takovému přiřazení, které používá prvků ze dvou různých množin, budeme říkat *vnější operace*. (Přesnou definici vyslovíme později.) Prvky z tělesa $\mathcal{T}$ budeme ve vztahu k maticím nazývat také *skaláry*.

**Definice 4.6** *Nechť* $c \in \mathcal{T}$, $A = ||a_{ij}|| \in M_{m\times n}(\mathcal{T})$. *Potom* (levým) součinem skaláru $c$ a matice $A$ *rozumíme matici* $cA = ||ca_{ij}|| \in M_{m\times n}(\mathcal{T})$.

`Poznámka`: Podobně je možno definovat pravý součin matice $A$ a skaláru $c$ vztahem $Ac = ||a_{ij}c||$. Ovšem vždy platí $ca_{ij} = a_{ij}c$, proto $Ac = cA$.

**Příklad 4.4** Je-li $c = 5$,

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

pak

$$cA = 5\begin{pmatrix} 2 & 3 & -1 \\ -2 & 0 & 4 \end{pmatrix} = \begin{pmatrix} 10 & 15 & -5 \\ -10 & 0 & 20 \end{pmatrix}.$$

**Věta 4.3** *Pro libovolné skaláry $c, d \in \mathcal{T}$ a libovolné matice $A, B \in M_{m\times n}$ platí*

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

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

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

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

D ů k a z: Nechť $c, d \in \mathcal{T}$, $A = ||a_{ij}||, B = ||b_{ij}|| \in M_{m\times n}(\mathcal{T})$. Potom platí:

1) $c(A + B) = c(||a_{ij}|| + ||b_{ij}||) = c||a_{ij} + b_{ij}|| = ||c(a_{ij} + b_{ij})|| = ||ca_{ij} + cb_{ij}|| = ||ca_{ij}|| + ||cb_{ij}|| = c||a_{ij}|| + c||b_{ij}|| = cA + cB$;

2) $(c+d)A = (c+d)||a_{ij}|| = ||(c+d)a_{ij}|| = ||ca_{ij} + da_{ij}|| = ||ca_{ij}|| + ||da_{ij}|| = c||a_{ij}|| + d||a_{ij}|| = cA + dA$;

3) $(cd)A = (cd)||a_{ij}|| = ||(cd)a_{ij}|| = ||c(da_{ij})|| = c||da_{ij}|| = c(d||a_{ij}||) = c(dA)$;

4) $1 \cdot A = 1 \cdot ||a_{ij}|| = ||1 \cdot a_{ij}|| = ||a_{ij}|| = A$.

□

V dalším budeme definovat součin matic. Na rozdíl od sčítání matic, které bylo operací na množině matic téhož typu, při násobení matic přiřazujeme dvěma maticím, na jejichž typy bude dán jistý požadavek, třetí matici, jejíž typ se nemusí rovnat typu žádné z původních matic, ale přitom bude těmito typy jednoznačně určen.

Než však přistoupíme k samotné definici součinu matic, popišme si metodu zkráceného zapisování součtů, kterou budeme při násobení matic s výhodou používat. Této metody je možno využít v libovolném komutativním okruhu.

Nechť $\mathcal{M} = (M, +, \cdot)$ je komutativní okruh. Pro stručné zapisování vzorců a výpočtů bude výhodné zapisovat součty pomocí tzv. *součtových znamének*. Jsou-li $a_1, a_2, \ldots, a_n$ prvky z $M$, $n \in \mathbb{N}$, pak budeme psát

$$a_1 + a_2 + \ldots + a_n = \sum_{i=1}^{n} a_i.$$

Číslo $i$ ve výrazu $a_i$ nazveme *součtový index*. Symbol $\sum\limits_{i=1}^{n}$ vyjadřuje, že postupně máme do $a_i$ dosazovat za index $i$ čísla $1, \ldots, n$ a vzniklé výrazy sečíst. Číslo 1 se nazývá *dolní mez*, číslo $n$ *horní mez* sčítání. Vidíme tedy, že nezáleží na tom, jakého symbolu použijeme k označení součtového indexu, protože za něj pouze dosazujeme čísla $1, \ldots, n$. Proto platí

$$\sum_{i=1}^{n} a_i = \sum_{k=1}^{n} a_k.$$

Protože nemusíme vždy pracovat jenom se součty, v nichž by se musel vyskytovat prvek $a_1$, nemusí být dolní mez rovna jenom číslu 1. Např. jsou-li $m, n \in \mathbb{N}$, $m < n$, pak píšeme

$$a_{m+1} + a_{m+2} + \ldots + a_n = \sum_{i=m+1}^{n} a_i.$$

Stejný součet můžeme také zapsat ve tvaru

$$a_{m+1} + a_{m+2} + \ldots + a_n = \sum_{i=1}^{n-m} a_{m+i}.$$

Jsou-li $m, n \in \mathbb{N}$, pak z asociativnosti sčítání v okruhu $\mathcal{M}$ platí

$$\sum_{i=1}^{m} a_i + \sum_{i=m+1}^{n} a_i = \sum_{i=1}^{m+n} a_i,$$

a protože sčítání v $\mathcal{M}$ je navíc komutativní, platí také

$$\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i = \sum_{i=1}^{n} (a_i + b_i).$$

Je-li $c \in M$, pak píšeme

$$c(a_1 + a_2 + \ldots + a_n) = c \sum_{i=1}^{n} a_i,$$

a na základě distributivnosti násobení vzhledem ke sčítání platí

$$c \sum_{i=1}^{n} a_i = \sum_{i=1}^{n} c a_i.$$

V poslední rovnosti vidíme, že prvek ve výrazu za součtovým znaménkem, který nezávisí na součtovém indexu, se v jednotlivých sčítancích nemění. Můžeme-li proto vyjádřit každý člen součtu ve tvaru takového součinu, že jeden z jeho činitelů je pro všechny sčítance stejný a nezávisí na součtovém indexu, můžeme tento činitel vytknout před součtové znaménko. Platí tedy

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m}\left(a_i \sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m}\left(\sum_{j=1}^{n} a_i b_j\right),$$

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \left(\sum_{j=1}^{n} b_j\right)\left(\sum_{i=1}^{m} a_i\right) =$$

$$= \sum_{j=1}^{n}\left(b_j \sum_{i=1}^{m} a_i\right) = \sum_{j=1}^{n}\left(\sum_{i=1}^{m} b_j a_i\right) = \sum_{j=1}^{n}\left(\sum_{i=1}^{m} a_i b_j\right).$$

Můžeme proto zbytečné závorky vynechat a psát

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j = \sum_{j=1}^{n}\sum_{i=1}^{m} a_i b_j.$$

Nechť $m, n \in \mathbb{N}$. Uvažujme $mn$ prvků $a_{ij} \in T$, $i = 1, \ldots, m$, $i = 1, \ldots, n$. Vytvoříme-li součty

$$\sum_{j=1}^{n} a_{ij}, i = 1, \ldots, m,$$

a sečteme-li tyto součty, dostaneme prvek

$$\sum_{i=1}^{m}\left(\sum_{j=1}^{n} a_{ij}\right).$$

Podobně, vytvoříme-li součty

$$\sum_{i=1}^{m} a_{ij}, j = 1, \ldots, n,$$

a sečteme-li je, dostaneme prvek

$$\sum_{j=1}^{n} \left( \sum_{i=1}^{m} a_{ij} \right).$$

Je zřejmé, že na základě asociativnosti a komutativnosti sčítání v okruhu $\mathcal{M}$ platí, že se tyto dva prvky sobě rovnají; můžeme tedy psát bez závorek

$$\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} = \sum_{j=1}^{n} \sum_{j=1}^{m} a_{ij}.$$

Budeme proto analogické dvojnásobné součty chápat tak, že nejdříve vždy vytvoříme vnitřní součty a potom takto získané součty sečteme v mezích vnějšího součtu. Musíme ovšem dbát na to, aby horní a dolní mez jednoho sčítání nebyla závislá na součtovém indexu druhého sčítání.

Nyní už můžeme součin matic definovat.

**Definice 4.7** *Nechť* $A = ||a_{ij}|| \in M_{m \times n}(\mathcal{T})$, $B = ||b_{jk}|| \in M_{n \times p}(\mathcal{T})$. *Potom* součinem *matic* $A$ a $B$ *(v tomto pořadí) 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* $i = 1, \ldots, m$, $k = 1, \ldots, p$.

`Poznámka:`

a) Vidíme tedy, že matice $A$ a $B$ můžeme násobit jenom tehdy, je-li počet sloupců matice $A$ stejný jako počet řádků matice $B$.

b) Existence součinu $AB$ ještě neimplikuje existenci součinu $BA$. Je zřejmé, že je-li $A \in M_{m \times n}(\mathcal{T})$, $B \in M_{n \times p}(\mathcal{T})$, pak $BA$ existuje právě tehdy, když $m = p$.

**Příklad 4.5** Jestliže

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

pak součin $AB$ existuje a platí

$$AB = \begin{pmatrix} 11 & -5 & 3 & 2 \\ 7 & 0 & 6 & -1 \end{pmatrix}$$

a přitom součin $BA$ neexistuje.

**Věta 4.4** *Násobení matic je asociativní, tj. jsou-li $A \in M_{m\times n}(\mathcal{T})$, $B \in M_{n\times p}(\mathcal{T})$, $C \in M_{p\times r}(\mathcal{T})$, pak*

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

D ů k a z: Nechť $A = ||a_{ij}||_{m\times n}$, $B = ||b_{jk}||_{n\times p}$, $C = ||c_{kl}||_{p\times r}$. Označme $AB = D = ||d_{ik}||_{m\times p}$, $BC = F = ||f_{jl}||_{n\times r}$. Podle definice součinu matic tedy platí

$$d_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk},\ \ f_{jl} = \sum_{k=1}^{p} b_{jk}c_{kl}.$$

Vypočítejme prvky matic $(AB)C$ a $A(BC)$, které leží na průsečíku $i$-tého řádku a $l$-tého sloupce.

Pro matici $(AB)C$ dostaneme prvek

$$\sum_{k=1}^{p} d_{ik}c_{kl} = \sum_{k=1}^{p}\left(\sum_{j=1}^{n} a_{ij}b_{jk}\right)c_{kl} = \sum_{k=1}^{p}\sum_{j=1}^{n}(a_{ij}b_{jk})c_{kl}$$

a pro matici $A(BC)$ prvek

$$\sum_{j=1}^{n} a_{ij}f_{jl} = \sum_{j=1}^{n} a_{ij}\left(\sum_{k=1}^{p} b_{jk}c_{kl}\right) = \sum_{j=1}^{n}\sum_{k=1}^{p} a_{ij}(b_{jk}c_{kl}).$$

Protože sčítání v tělese $\mathcal{T}$ je komutativní a asociativní a násobení v $\mathcal{T}$ je asociativní, oba tyto prvky se sobě rovnají, a proto z definice rovnosti matic dostáváme i rovnost $(AB)C = A(BC)$. □

`Poznámka`: Matici $(AB)C = A(BC)$ můžeme proto bez obav z nedorozumění označovat také $ABC$.

**Příklad 4.6** Nechť

$$A = \begin{pmatrix} 5 & 2 \\ -1 & 1 \end{pmatrix}, B = \begin{pmatrix} -3 & 1 \\ 2 & -4 \end{pmatrix}, C = \begin{pmatrix} 0 & -2 \\ -3 & 1 \end{pmatrix}.$$

Potom matici $ABC$ můžeme např. určit takto:

$$ABC = (AB)C = \left[\begin{pmatrix} 5 & 2 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} -3 & 1 \\ 2 & -4 \end{pmatrix}\right]\begin{pmatrix} 0 & -2 \\ -3 & 1 \end{pmatrix} =$$
$$\begin{pmatrix} -11 & -3 \\ 5 & -5 \end{pmatrix}\begin{pmatrix} 0 & -2 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} 9 & 19 \\ 15 & -15 \end{pmatrix}.$$

Přitom pro kontrolu spočítáme také matici $A(BC)$. Platí

$$A(BC) = \begin{pmatrix} 5 & 2 \\ -1 & 1 \end{pmatrix} \left[ \begin{pmatrix} -3 & 1 \\ 2 & -4 \end{pmatrix} \begin{pmatrix} 0 & -2 \\ -3 & 1 \end{pmatrix} \right] = \begin{pmatrix} 5 & 2 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} -3 & 7 \\ 12 & -8 \end{pmatrix} = \begin{pmatrix} 9 & 19 \\ 15 & -15 \end{pmatrix}.$$

**Věta 4.5** *Násobení matic je distributivní vzhledem ke sčítání, tj. jsou-li $A \in M_{m\times n}(\mathcal{T})$, $B, C \in M_{n\times p}(\mathcal{T})$, pak $A(B+C) = AB + AC$, a jsou-li $B, C \in M_{n\times p}(\mathcal{T})$ a $D \in M_{p\times r}(\mathcal{T})$, pak $(B+C)D = BD + CD$.*

D ů k a z: Nechť $A = ||a_{ij}||_{m\times n}$, $B = ||b_{jk}||_{n\times p}$, $C = ||c_{jk}||_{n\times p}$. Označme $A(B+C) = F = ||f_{ik}||_{m\times p}$, $AB + AC = G = ||g_{ik}||_{m\times p}$. Platí

$$f_{ik} = \sum_{j=1}^{n} a_{ij}(b_{jk} + c_{jk}) = \sum_{j=1}^{n} (a_{ij}b_{jk} + a_{ij}c_{jk}) = g_{ik},$$

což ovšem znamená, že $A(B+C) = AB + AC$.

Rovnost $(B+C)D = BD + CD$ se dokáže analogicky. □

**Věta 4.6** *Je-li $n \in \mathbb{N}$, pak $\mathcal{M}_n(\mathcal{T}) = (M_n(\mathcal{T}), +, \cdot)$ je okruh s jednotkovým prvkem. Je-li $n > 1$, pak $\mathcal{M}_n(\mathcal{T})$ není komutativní a obsahuje netriviální dělitele nuly. Je-li $n = 1$, pak $\mathcal{M}_n(\mathcal{T})$ je komutativní těleso.*

D ů k a z: Podle věty 4.2 platí, že $(M_n(\mathcal{T}), +)$ je komutativní grupa a podle definice součinu matic a věty 4.4 je $(M_n(\mathcal{T}), \cdot)$ pologrupa. Je zřejmé, že jednotkovým prvkem v $(M_n(\mathcal{T}), \cdot)$ je jednotková matice $E_n$. Podle věty 4.5 je násobení matic oboustranně distributivní vzhledem ke sčítání matic. To ovšem znamená, že $\mathcal{M}_n(\mathcal{T}) = (M_n(\mathcal{T}), +, \cdot)$ je okruh.

Nechť $n > 1$. Uvažujme např. matice $A_1, A_2 \in M_n(\mathcal{T})$, kde

$$A_1 = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & 0 & \cdots & 1 \\ 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Pak platí

$$A_1A_2 = \begin{pmatrix} 0 & 0 & \cdots & 0 & n \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}, A_2A_1 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

tedy $A_1A_2 \neq A_2A_1$, a proto okruh $\mathcal{M}_n(\mathcal{T})$ není komutativní. Současně ovšem vidíme, že $A_2A_1 = N$, což znamená, že $A_2$ je levým a $A_1$ pravým netriviálním dělitelem nuly.

Nechť $n = 1$. Pak $||a_{11}|| + ||b_{11}|| = ||a_{11} + b_{11}||$, $||a_{11}|| \cdot ||b_{11}|| = ||a_{11}b_{11}||$, takže sčítání i násobení v $\mathcal{M}_1(\mathcal{T})$ odpovídá těmto operacím v $\mathcal{T}$ (pokud matici $||x_{11}||$ ztotožníme s prvkem $x_{11}$). To znamená, že $\mathcal{M}_1(\mathcal{T})$ je také komutativní těleso. □

## 4.2 Aritmetické vektorové prostory

Nyní si blíže všimneme takových matic nad číselným tělesem $\mathcal{T}$, které mají buď jen jeden řádek nebo jen jeden sloupec. V analytické geometrii na střední škole se každému geometrickému vektoru v rovině přiřazuje uspořádaná dvojice reálných čísel, tzv. souřadnice tohoto vektoru. Podobně každému vektoru třírozměrného prostoru je přiřazena uspořádaná trojice jeho souřadnic. Přitom každý vektor je svými souřadnicemi plně určen, proto každou uspořádanou dvojici, resp. trojici, reálných čísel můžeme samu považovat za tzv. aritmetický vektor. Podobným způsobem můžeme definovat vektory jakéhokoliv konečného rozměru. Použijeme k tomu výsledků, které jsme obecně odvodili pro matice.

**Definice 4.8** *Pro každé $n \in \mathbb{N}$ budeme (*řádkovým*) $n$-*rozměrným aritmetickým vektorovým prostorem nad $\mathcal{T}$ *(značíme $\mathcal{T}^n$) rozumět komutativní grupu $(M_{1\times n}(\mathcal{T}), +)$ všech matic typu $1 \times n$ nad $\mathcal{T}$ uvažovanou spolu s násobením matic z $M_{1\times n}(\mathcal{T})$ skaláry z $\mathcal{T}$. Každou matici z $M_{1\times n}(\mathcal{T})$ pak nazveme* $n$-rozměrný *(*řádkový*)* aritmetický vektor nad $\mathcal{T}$.

`Poznámka:`

a) Pro označení vektorů budeme místo velkých písmen používaných pro matice užívat malá podtržená písmenka, nebo standardně používanou šipku. Je-li $\overrightarrow{u} = (u_1, \ldots, u_n)$ $n$-rozměrný aritmetický vektorový vektor, pak prvky $u_1, \ldots, u_n \in \mathcal{T}$ budeme nazývat *souřadnice vektoru* $\overrightarrow{u}$.

b) Podobně budeme za vektory považovat matice typu $n \times 1$ nad $\mathcal{T}$. Pro odlišení od řádkových vektorů z $\mathcal{T}^n$ je budeme nazývat *sloupcové aritmetické vektory nad* $\mathcal{T}$ a k jejich označení použijeme zápisu užívaného pro transponované matice, např.

$$\overrightarrow{u}^T = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}.$$

Komutativní grupu $(M_{n\times 1}(\mathcal{T}), +)$ spolu s násobením vektorů skaláry nazýváme *sloupcový n-rozměrný aritmetický vektorový prostor nad* $\mathcal{T}$ a značíme jej $(\mathcal{T}^n)^T$.

c) V dalším si budeme všímat jen řádkových vektorů. Všechny pojmy a vlastnosti je možno samozřejmě bezprostředně převést i pro případ sloupcových vektorů.

**Definice 4.9** *Jsou-li $\overrightarrow{v}, \overrightarrow{u_1}, \ldots, \overrightarrow{u_k}$ aritmetické vektory z $\mathcal{T}^n$, potom řekneme, že vektor $\overrightarrow{v}$ je* lineární kombinací vektorů $\overrightarrow{u_1}, \ldots, \overrightarrow{u_k}$*, existují-li čísla $c_1, \ldots, c_k \in \mathcal{T}$ taková, že*

$$\overrightarrow{v} = c_1\overrightarrow{u_1} + \ldots + c_k\overrightarrow{u_k} = \sum_{i=1}^{k} c_i\overrightarrow{u_i}.$$

Víme, že dvě matice téhož typu se sobě rovnají, pokud se na všech místech rovnají jejich odpovídající si prvky. Proto také bude platit, že pokud $\overrightarrow{v} = (v_1, \ldots, v_n)$, $\overrightarrow{u_1} = (u_{11}, \ldots, u_{1n})$, $\overrightarrow{u_2} = (u_{21}, \ldots, u_{2n})$, …, $\overrightarrow{u_k} = (u_{k1}, \ldots, u_{kn})$, pak vektorová rovnost

$$\overrightarrow{v} = c_1\overrightarrow{u_1} + c_2\overrightarrow{u_2} + \ldots + c_k\overrightarrow{u_k}$$

nastává právě tehdy, platí-li soustava $n$ číselných rovností

$$\begin{array}{ccccccccc} v_1 & = & u_{11}c_1 & + & u_{21}c_2 & + & \dots & + & u_{k1}c_k \\ v_2 & = & u_{12}c_1 & + & u_{22}c_2 & + & \dots & + & u_{k2}c_k \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ v_n & = & u_{1n}c_1 & + & u_{2n}c_2 & + & \dots & + & u_{kn}c_k \end{array}.$$

**Příklad 4.7** Zjistěte, je-li vektor $\overrightarrow{v}$ lineární kombinací vektorů $\overrightarrow{u_1}, \overrightarrow{u_2}, \overrightarrow{u_3}$. ($\overrightarrow{v}, \overrightarrow{u_1}, \overrightarrow{u_2}, \overrightarrow{u_3} \in \mathcal{R}^3$.)

a) $\overrightarrow{v} = (4, -2, 3), \overrightarrow{u_1} = (2, 1, -2), \overrightarrow{u_2} = (-3, 4, 2), \overrightarrow{u_3} = (1, 0, -3)$

b) $\overrightarrow{v} = (2, -1, 3), \overrightarrow{u_1} = (-5, 2, 1), \overrightarrow{u_2} = (1, -3, 2), \overrightarrow{u_3} = (-3, -4, 5)$

Máme tedy zjistit, zdali existují reálná čísla $c_1, c_2, c_3$ taková, aby platilo

$$\overrightarrow{v} = \sum_{i=1}^{3} c_i \overrightarrow{u_i},$$

tzn. zjistíme, má-li řešení soustava rovnic

a)

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

Eliminační metodou vypočítáme, že tato soustava má jediné řešení $c_1 = 2, c_2 = -1, c_3 = -3$ tedy $\overrightarrow{v} = 2\overrightarrow{u_1} - \overrightarrow{u_2} - 3\overrightarrow{u_3}$, a proto $\overrightarrow{v}$ je lineární kombinací vektorů $\overrightarrow{u_1}, \overrightarrow{u_2}, \overrightarrow{u_3}$.

b)

$$\begin{array}{rcrcrcr} -5c_1 & + & c_2 & - & 3c_3 & = & 2 \\ 2c_1 & - & 3c_2 & - & 4c_3 & = & -1. \\ c_1 & + & 2c_2 & + & 5c_3 & = & 3 \end{array}$$

Snadno vypočítáme, že tato soustava nemá řešení, tzn. že vektor $\overrightarrow{v}$ není lineární kombinací vektorů $\overrightarrow{u_1}, \overrightarrow{u_2}, \overrightarrow{u_3}$.

`Poznámka:`

a) Protože pro každý vektor $\overrightarrow{v} \in \mathcal{T}^n$ platí $\overrightarrow{v} = 1 \cdot \overrightarrow{v}$, je každý vektor svou lineární kombinací.

b) Nulový vektor $\overrightarrow{o} = (0, 0, \dots, 0)$ je lineární kombinací libovolných vektorů $\overrightarrow{u_1}, \dots, \overrightarrow{u_k}$, protože vždy platí mj.

$$\overrightarrow{o} = 0\overrightarrow{u_1} + 0\overrightarrow{u_2} + \dots + 0\overrightarrow{u_k}$$

**Definice 4.10**

*a) Lineární kombinaci* $\sum_{i=1}^{k} 0\overrightarrow{u_i}$ *vektorů* $\overrightarrow{u_1}, \dots, \overrightarrow{u_k}$ *nazveme* triviální nulovou kombinací *vektorů* $\overrightarrow{u_1}, \dots, \overrightarrow{u_k}$.

b) *Každou lineární kombinaci* $\sum_{i=1}^{k} c_i \overrightarrow{u_i}$, *která je rovna nulovému vektoru* $\overrightarrow{o}$ *a v níž alespoň jeden z koeficientů* $c_1, \dots, c_k$ *je nenulový, nazveme* netriviální nulová kombinace *vektorů* $\overrightarrow{u_1}, \dots, \overrightarrow{u_k}$.

**Příklad 4.8** Označme $\overrightarrow{u_1} = (-3, 1, 2), \overrightarrow{u_2} = (5, 3, -3), \overrightarrow{u_3} = (-4, 6, 3)$. Potom $0\overrightarrow{u_1} + 0\overrightarrow{u_2} + 0\overrightarrow{u_3}$ je triviální nulová kombinace a $3\overrightarrow{u_1} + 3\overrightarrow{u_2} - \overrightarrow{u_3}$ je netriviální nulová kombinace těchto vektorů.

**Definice 4.11** *Jsou-li* $\overrightarrow{u_1}, \dots, \overrightarrow{u_k}$ *vektory z* $\mathcal{T}^n$, *pak řekneme, že tyto vektory jsou*

a) lineárně závislé, *existuje-li alespoň jedna jejich netriviální nulová kombinace;*

b) lineárně nezávislé, *jestliže jedinou jejich nulovou lineární kombinací je kombinace triviální.*

`Poznámka`: Je zřejmé, že vektory $\overrightarrow{u_1} = (u_{11}, \dots, u_{1n})$, $\overrightarrow{u_2} = (u_{21}, \dots, u_{2n})$, ..., $\overrightarrow{u_k} = (u_{k1}, \dots, u_{kn})$ jsou lineárně závislé právě tehdy, má-li soustava číselných rovnic

$$\begin{array}{ccccccccc} 0 & = & u_{11}c_1 & + & u_{21}c_2 & + & \dots & + & u_{k1}c_k \\ 0 & = & u_{11}c_1 & + & u_{21}c_2 & + & \dots & + & u_{k1}c_k \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ 0 & = & u_{1n}c_1 & + & u_{2n}c_2 & + & \dots & + & u_{kn}c_k \end{array}$$

aspoň jedno nenulové řešení (tj. takové řešení, v němž je alespoň jedno z čísel $c_1, \dots, c_k$ různé od nuly).

**Příklad 4.9** Zjistěte, jsou-li lineárně závislé nebo nezávislé vektory

a) $\overrightarrow{u_1} = (2, -3), \overrightarrow{u_2} = (1, 4), \overrightarrow{u_3} = (4, -17)$;

b) $\overrightarrow{u_1} = (-2, 4, 1), \overrightarrow{u_2} = (5, 0, -3)$.

a) Protože soustava

$$\begin{array}{rcrcrcl} 2c_1 & + & c_2 & + & 4c_3 & = & 0 \\ -3c_1 & + & 4c_2 & + & -17c_3 & = & 0 \end{array}$$

má např. řešení $c_1 = -3, c_2 = 2, c_3 = 1$, jsou vektory $\overrightarrow{u_1}, \overrightarrow{u_2}, \overrightarrow{u_3}$ lineárně závislé.

b) Soustava

$$\begin{array}{rcrcl} -2c_1 & + & 5c_2 & = & 0 \\ 4c_1 & & & = & 0 \\ c_1 & - & 3c_2 & = & 0 \end{array}$$

nemá řešení, v němž by $c_1$ nebo $c_2$ bylo různé od nuly, tedy vektory $\overrightarrow{u_1}, \overrightarrow{u_2}$ jsou lineárně závislé.

## 4.3 Cvičení

**4.1** Nad tělesem $\mathbb{R}$ jsou dány matice

$$A=\begin{pmatrix} 2 & 3 & -7 \\ 1 & -1 & 0 \end{pmatrix}, B=\begin{pmatrix} -1 & 0 & 4 \\ 7 & 15 & -10 \end{pmatrix}, C=\begin{pmatrix} 5 & 11 \\ 2 & -1 \end{pmatrix}, D=\begin{pmatrix} 11 & 4 & 0 \\ 2 & -3 & 6 \end{pmatrix}.$$

Určete zda jsou definovány matice $A+B, A\cdot B, B\cdot A, C+D, C\cdot D, D\cdot C$, v kladném případě je určete.

[ $\begin{pmatrix} 1 & 3 & -3 \\ 8 & 14 & -10 \end{pmatrix}$; ne; ne; ne; $\begin{pmatrix} 77 & -13 & 66 \\ 20 & 11 & -6 \end{pmatrix}$; ne ]

**4.2** Určete matici $2A+B-3C$, platí-li

$$A=\begin{pmatrix} 2 & 3 & -1 & 5 \\ 8 & -4 & 0 & -7 \end{pmatrix}, B=\begin{pmatrix} -5 & 2 & 1 & -6 \\ 1 & -10 & 2 & -3 \end{pmatrix}, C=\begin{pmatrix} -4 & 2 & 0 & 1 \\ 3 & 8 & -6 & 4 \end{pmatrix}.$$

[ $\begin{pmatrix} 11 & 2 & -1 & 7 \\ 8 & -42 & 20 & -5 \end{pmatrix}$ ]

**4.3** Nad tělesem $\mathbb{Z}_7$ určete součet $A+B+C$ matic

$$A=\begin{pmatrix} 1 & 3 & 4 \\ 5 & 6 & 0 \\ 3 & 4 & 2 \end{pmatrix}, B=\begin{pmatrix} 0 & 1 & 6 \\ 5 & 4 & 2 \\ 3 & 1 & 5 \end{pmatrix}, C=\begin{pmatrix} 3 & 2 & 0 \\ 4 & 6 & 1 \\ 5 & 2 & 3 \end{pmatrix}.$$

[ $\begin{pmatrix} 4 & 6 & 3 \\ 0 & 2 & 3 \\ 4 & 0 & 3 \end{pmatrix}$ ]

**4.4** Nad tělesem $\mathbb{R}$ řešte maticovou rovnici

$$2\cdot\begin{pmatrix} 2 & 5 & 0 \\ 7 & -1 & 3 \end{pmatrix} + 3\cdot X = 7\cdot\begin{pmatrix} 2 & 5 & 0 \\ 7 & -1 & 3 \end{pmatrix} + \begin{pmatrix} -1 & 2 & 6 \\ -2 & 5 & 0 \end{pmatrix}.$$

[ $X=\begin{pmatrix} 3 & 9 & 2 \\ 11 & 0 & 5 \end{pmatrix}$ ]

**4.5** Vypočítejte

$$\text{a)}\begin{pmatrix} 4 & -1 \\ 5 & -2 \end{pmatrix}^5;\ \text{b)}\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}^n.$$

[ a)$\begin{pmatrix} 304 & -61 \\ 305 & -62 \end{pmatrix}$; b)$\begin{pmatrix} \lambda^n & n\lambda^{n-1} \\ 0 & \lambda^n \end{pmatrix}$ ]

**4.6** Nalezněte vzorec pro výpočet $A^n$ kde $n\in\mathbb{N}$ a $A$ je matice nad tělesem $\mathbb{R}$:

$$A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}.$$

Nalezený vzorec ověřte matematickou indukcí.
[ $\begin{pmatrix} \cos n\alpha & -\sin n\alpha \\ \sin n\alpha & \cos n\alpha \end{pmatrix}$ ]

**4.7** Určete $A^3$ kde matice $A$ je $n$-tého stupně

$$A = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}^3.$$

[ $\begin{pmatrix} 1 & 3 & 6 & \cdots & \frac{n(n+1)}{2} \\ 0 & 1 & 3 & \cdots & \frac{(n-1)n}{2} \\ 0 & 0 & 1 & \cdots & \frac{(n-2)(n-1)}{2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$ ]

**4.8** Vyšetřete strukturu $\mathcal{M} = (M, +, \cdot)$ kde $M = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix}; a, b \in \mathbb{Z}_3 \right\}$, operace $+, \cdot$ jsou operace sčítání a násobení matic. Zapište množinu $M$ výčtem prvků.
[ komutativní těleso ]

**4.9** Matice $A, B$ nazýváme *zaměnitelné*, existují-li oba součiny $A \cdot B$ a $B \cdot A$ a platí-li $A \cdot B = B \cdot A$. Zřejmě zaměnitelné matice jsou čtvercové a mají stejný stupeň. Určete všechny matice, které jsou zaměnitelné s maticí

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

[ $\begin{pmatrix} a & 4b-4a \\ 3a-3b & b \end{pmatrix}$, kde $a, b \in \mathbb{R}$ ]

**4.10** Určete všechny matice, které jsou zaměnitelné s každou diagonální maticí $n$-tého stupně.
[ Právě všechny diagonální matice $n$-tého stupně. ]

**4.11** Zjistěte, je-li levým, popř. pravým, netriviálním dělitelem nuly matice
$a) \begin{pmatrix} 2 & -3 \\ -6 & 9 \end{pmatrix}, \quad b) \begin{pmatrix} 5 & 2 \\ -1 & 7 \end{pmatrix}.$
[ a) levý i pravý dělitel nuly; b) není ani levý ani pravý dělitel nuly ]

**4.12** Určete vektor $\overrightarrow{\xi}$ z rovnice $3\overrightarrow{u_1} - 2\overrightarrow{u_2} + 4\overrightarrow{u_3} + 2\overrightarrow{\xi} = \overrightarrow{0}$ kde $\overrightarrow{u_1} = (2,-2,4,6)$, $\overrightarrow{u_2} = (4,-5,2,6)$, $\overrightarrow{u_3} = (4,-1,-5,-3)$.
[ $(-7,0,6,3)$ ]

**4.13** Rozhodněte jsou-li následující vektory mezi sebou lin. závislé nebo lin. nezávislé

a) $\overrightarrow{u_1} = (2,3,-1), \overrightarrow{u_2} = (4,5,2)$;

b) $\overrightarrow{u_1} = (-3,2,4), \overrightarrow{u_2} = (1,5,-2), \overrightarrow{u_3} = (2,-4,3)$;

c) $\overrightarrow{u_1} = (2,-6,4), \overrightarrow{u_2} = (-1,2,-4), \overrightarrow{u_3} = (4,-9,14)$.

[ a), b) lineárně nezávislé; c) lineárně závislé ]

# Kapitola 5

# Determinanty

## 5.1 Pořadí, permutace

Definice determinantu čtvercové matice s výhodou využívá permutací, s kterými jsme se již stručně setkali v části 2.4. Proto se nyní budeme nejdříve zabývat důkladnějším studiem permutací.

**Definice 5.1** *Je-li $A = \{a_1, a_2, \ldots, a_n\}$, kde $n \geq 1$, konečná množina, potom* pořadím *množiny $A$ nazveme libovolnou posloupnost*

$$\pi = (a_{k_1}, a_{k_2}, \ldots, a_{k_n})$$

*prvků z $A$ takovou, že každý prvek z množiny $A$ se v $\pi$ vyskytuje právě jednou.*

**Věta 5.1** *Pro každou $n$-prvkovou množinu ($n \geq 1$) existuje právě $n!$ pořadí.*

D ů k a z: Matematickou indukcí vzhledem k počtu $n$ prvků množiny. Zřejmě pro $n = 1$ tvrzení platí. Předpokládejme, že $n > 1$ a že pro každou $(n-1)$-prvkovou množinu existuje právě $(n-1)!$ pořadí. Je-li $A = \{a_1, a_2, \ldots, a_n\}$ $n$-prvková množina, pak počet pořadí množiny $A$, která mají na prvním místě prvek $a_i$ $(i = 1, \ldots, n)$, je roven počtu pořadí $(n-1)$-prvkové množiny $\{a_1, a_2, \ldots, a_n\} \setminus \{a_i\}$, a těch je podle indukčního předpokladu $(n-1)!$. Tedy všech pořadí na množině $A$ je $n(n-1)! = n!$. □

Pro další úvahy bude nejpřehlednější, když pro každé $n \geq 1$ budeme standardně pracovat s množinou $A = \{1, 2, \ldots, n\}$.

**Definice 5.2** Základním pořadím *na množině $A = \{1, 2, \ldots, n\}$ rozumíme pořadí $\pi = (1, 2, \ldots, n)$.*

Připomeňme si ještě, že permutací na množině $A$ rozumíme každou bijekci $A$ na $A$ a že je-li $P$ permutace na $A$, pak ji můžeme zapsat ve tvaru schématu

$$P = \begin{pmatrix} i_1 & i_2 & \ldots & i_n \\ P(i_1) & P(i_2) & \ldots & P(i_n) \end{pmatrix}.$$

Tedy permutaci je možno vlastně zapsat pomocí dvou pořadí, což také budeme stručně zapisovat

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

Je zřejmé, že dostaneme jen jiný zápis stejné permutace, jestliže zapíšeme v některém jiném pořadí současně prvky v prvním řádku i jejich obrazy ve druhém řádku.

**Příklad 5.1**

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

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

Nejčastěji budeme pracovat s takovými zápisy permutací, ve kterých bude horní řádek v základním pořadí. Např. permutaci $P$ z příkladu 5.1 pak zapíšeme ve tvaru

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

Tomuto tvaru budeme někdy také říkat *základní tvar permutace*.

**Věta 5.2** *Pro každou $n$-prvkovou množinu ($n \leq 1$) existuje právě $n!$ permutací.*

D ů k a z: Víme, že každou permutaci můžeme zapsat v základním tvaru. To ovšem znamená, že počet permutací na $n$-prvkové množině bude stejný jako počet pořadí na této množině, protože právě tolik bude také permutací v základním tvaru. Z věty 5.1 dostáváme tvrzení. □

Všechny zápisy téže permutace budou pro naše účely rovnocenné, protože mají stejnou charakteristickou vlastnost, tzv. znaménko permutace. Nejdřív ale budeme definovat znaménko pořadí.

**Definice 5.3** *Je-li $\pi = (k_1, k_2, \ldots, k_n)$ pořadí, pak řekneme, že prvky $k_i$ a $k_j$* tvoří *v pořadí $\pi$* inverzi, *platí-li $i < j$ a $k_i > k_j$.*

**Příklad 5.2** Je-li $\pi = (2, 4, 3, 5, 1)$, pak inverze tvoří právě dvojice prvků

$$2, 1; 4, 3; 4, 1; 3, 1; 5, 1.$$

Je-li $\pi$ pořadí, pak počet inverzí v $\pi$ označíme $[\pi]$.

**Definice 5.4** Znaménkem pořadí *$\pi$ rozumíme číslo $sgn\ \pi = (-1)^{[\pi]}$. Je-li $sgn\ \pi = 1$, pak se pořadí $\pi$ nazývá* sudé, *je-li $sgn\ \pi = -1$, pak se $\pi$ nazývá* liché.

(Symbol $sgn\ \pi$ je zkratka latinského „signum“, což je „znamení“.)

**Příklad 5.3** Protože pořadí $\pi$ z příkladu 5.2 má 5 inverzí, je $sgn\ \pi = (-1)^5 = -1$, a tedy $\pi$ je liché.

Nyní se už dostáváme k pojmu znaménko permutace.

**Definice 5.5** Znaménkem permutace

$$P = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ k_1 & k_2 & \dots & k_n \end{pmatrix} = \begin{pmatrix} \pi_1 \\ \pi_2 \end{pmatrix}$$

*rozumíme číslo $sgn\ P$, které se rovná $+1$, platí-li $sgn\ \pi_1 = sgn\ \pi_2$, a rovná se $-1$, platí-li $sgn\ \pi_1 = -sgn\ \pi_2$.*

*Permutace $P$ se nazývá* sudá, *je-li $sgn\ P = 1$; v opačném případě se permutace $P$ nazývá* lichá.

**Příklad 5.4** Určete znaménko permutace

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

Vidíme, že $[\pi_1] = 3$ a $[\pi_2] = 5$, tzn., že $sgn\ \pi_1 = -1$, $sgn\ \pi_2 = -1$. Proto $sgn\ \pi_1 = sgn\ \pi_2$, což znamená, že $sgn\ P = +1$.

`Poznámka:` Je zřejmé, že základní pořadí je sudé, proto je-li permutace $P$ v základním tvaru, tj.

$$P = \begin{pmatrix} \pi_0 \\ \pi_2 \end{pmatrix},$$

pak $sgn\ P = sgn\ \pi_2$.

**Příklad 5.5** Upravíme-li permutaci $P$ z příkladu 5.4 do základního tvaru

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} = \begin{pmatrix} \pi_0 \\ \pi_2' \end{pmatrix},$$

pak $[\pi_2'] = 6$, tady $sgn\ P = sgn\ \pi_2' = 1$.

Označme identickou permutaci (pro připomenutí, je to taková permutace, která ponechává všechny prvky na místě) symbolem $P_0$. Připomeňme, že inverzní permutací k permutaci $P$ rozumíme takovou permutaci $P^{-1}$, že $P \circ P^{-1} = P_0 = P^{-1} \circ P$. Víme, že ke každé permutaci $P$ permutace $P^{-1}$ existuje a že je určena jednoznačně.

**Věta 5.3** *Pro každou permutaci $P$ platí $sgn\ P = sgn\ P^{-1}$.*

D ů k a z: Víme, že je-li $P = \begin{pmatrix} \pi_1 \\ \pi_2 \end{pmatrix}$, pak $P^{-1} = \begin{pmatrix} \pi_2 \\ \pi_1 \end{pmatrix}$. Tvrzení tedy plyne přímo z definice znaménka permutace. □

Pro studium permutací a determinantů mají velký význam tzv. transpozice.

**Definice 5.6** Transpozicí *na množině* $A = \{1, 2, \dots, n\}$ *nazýváme každou takovou permutaci* $P$ *na* $A$*, pro kterou existují čísla* $i, j \in A$, $i \neq j$*, taková, že* $P(k) = k$ *pro každé* $k \in A \setminus \{i, j\}$ *a* $P(i) = j$, $P(j) = i$.

Pokud bude zřejmý počet prvků množiny $A$, pak tuto transpozici budeme také stručně označovat $(i, j)$.

**Příklad 5.6** Permutace
$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$$
zaměňuje navzájem čísla 2 a 4 a ostatní ponechává na místě, proto $P$ je transpozicí $(2, 4)$ (resp. $(4, 2)$).

**Věta 5.4** *Každá transpozice je sama k sobě inverzní.*

D ů k a z: Plyne přímo z definice transpozice. □

**Definice 5.7** *Je-li* $\pi = (i_1, i_2, \dots, i_n)$ *pořadí a* $P = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$ *permutace na* $\{1, 2, \dots, n\}$*, pak řekneme, že pořadí* $\pi' = (k_{i_1}, k_{i_2}, \dots, k_{i_n})$ vznikne z pořadí $\pi$ pomocí permutace $P$.

**Příklad 5.7** Je-li $\pi = (2, 4, 5, 1, 3)$ a
$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix},$$
pak pořadí $\pi' = (4, 2, 3, 5, 1)$ vzniklo z pořadí $\pi$ pomocí permutace $P$.

**Věta 5.5** *Vznikne-li pořadí* $\pi'$ *z pořadí* $\pi$ *pomocí některé transpozice, pak platí*
$$sgn\ \pi' = -sgn\ \pi.$$

D ů k a z: Nechť $\pi = (k_1, k_2, \dots, k_n)$ je pořadí na množině $\{1, 2, \dots, n\}$, $n > 1$.

a) Nechť pořadí $\pi'$ vznikne z pořadí $\pi$ pomocí transpozice $(k_i, k_{i+1})$, kde $i \in \{1, 2, \dots, n-1\}$. Je zřejmé, že každá dvojice prvků $k_j, k_r$ $(j < r)$ různá od $k_i, k_{i+1}$ tvoří nebo netvoří inverzi současně v obou pořadích $\pi$ a $\pi'$. Tedy v případě, že $k_i, k_{i+1}$ tvoří v $\pi$ inverzi, platí $[\pi] = [\pi'] + 1$, a pokud $k_1, k_{i+1}$ netvoří v $\pi$ inverzi, platí $[\pi] = [\pi'] - 1$. V každém případě ovšem $sgn\ \pi' = -sgn\ \pi$.

b) Předpokládejme, že $\pi'$ vznikne z $\pi$ pomocí transpozice $(k_i, k_j)$, kde $i < j$. Tedy je-li
$$\pi = (k_1, \dots, k_{i-1}, k_i, k_{i+1}, \dots, k_{j-1}, k_j, k_{j+1}, \dots, k_n),$$
pak
$$\pi' = (k_1, \dots, k_{i-1}, k_j, k_{i+1}, \dots, k_{j-1}, k_i, k_{j+1}, \dots, k_n).$$

Přitom ovšem od $\pi$ k $\pi'$ můžeme přejít také postupným prováděním transpozic sousedních prvků. Provedeme-li nejdříve transpozice

$$(k_i, k_{i+1}), (k_i, k_{i+2}), \ldots, (k_i, k_j),$$

dostaneme pořadí

$$\pi'' = (k_1, \ldots, k_{i-1}, k_{i+1}, \ldots, k_{j-1}, k_i, k_j, k_{j+1}, \ldots, k_n),$$

a následným použitím transpozic

$$(k_j, k_{j-1}), (k_j, k_{j-2}), \ldots, (k_j, k_{i+1})$$

už dostaneme pořadí $\pi'$. Celkově tedy postupně používáme $(j-i)+[(j-i)-1] = 2(j-i)-1$ transpozic. Protože každá z transpozic sousedních prvků změní podle části a) znaménko pořadí, platí proto

$$sgn\ \pi' = (-1)^{2(j-i)-1} \cdot sgn\ \pi = -sgn\ \pi.$$

□

**Věta 5.6** *Všech $n!$ pořadí $n$-prvkové množiny $\{1, 2, \ldots, n\}$ je možno uspořádat do posloupnosti tak, že za první prvek posloupnosti zvolíme libovolné pořadí a každé další pořadí v posloupnosti vznikne z předchozího pomocí některé transpozice.*

D ů k a z: Provedeme indukcí podle počtu $n$ prvků množiny.

Pro $n = 1$ je tvrzení triviální.

Nechť tvrzení platí pro každou nejvýše $(n-1)$-prvkovou množinu a uvažujme $n$-prvkovou množinu $A = \{1, 2, \ldots, n\}$. Vybereme libovolné pořadí $(k_1, k_2, \ldots, k_n)$ množiny $A$. Podle indukčního předpokladu můžeme požadovaným způsobem uspořádat všech $(n-1)!$ pořadí množiny $\{k_2, \ldots, k_n\}$ počínaje pořadím $(k_2, k_3, \ldots, k_n)$. Napíšeme-li před první prvek každého z těchto pořadí množiny $\{k_2, \ldots, k_n\}$ prvek $k_1$, dostaneme posloupnost $(n-1)!$ pořadí množiny $\{1, 2, \ldots, n\}$, která postupně vznikají pomocí transpozic.

Nyní jako další prvek posloupnosti zařadíme pořadí, které vznikne z posledního pořadí dosud konstruované posloupnosti pomocí transpozice $(k_1, k_2)$ a provádíme stejné úvahy s pořadími na množině $\{k_1, k_2, \ldots, k_n\}$. Tímto způsobem postupujeme tak dlouho, až zapíšeme do posloupnosti všechna pořadí, která začínají prvkem $k_n$. □

**Věta 5.7** *Je-li $n \geq 2$, pak mezi všemi $n!$ pořadími $n$-prvkové množiny je právě $\frac{n!}{2}$ sudých a $\frac{n!}{2}$ lichých pořadí.*

D ů k a z: Uspořádáme-li všechna pořadí do konečné posloupnosti jako ve větě 5.6, pak podle věty 5.5 platí, že znaménka dvou po sobě jdoucích pořadí v této posloupnosti jsou různá. Odtud plyne tvrzení. □

Bez důkazu nyní uvedeme následující větu.

**Věta 5.8** *Každou permutaci je možno zapsat ve tvaru složení konečného počtu transpozic. Přitom platí, že sudá permutace se skládá ze sudého počtu a lichá permutace z lichého počtu transpozic.*

**Příklad 5.8** Rozložíme na transpozice permutaci

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

Platí $sgn\ P = -1$, proto podle věty 5.8 dostaneme rozklad na lichý počet transpozic. Protože horní řádek permutace můžeme vždy psát v základním pořadí, bude postačovat, ukážeme-li, pomocí jakých transpozic dostaneme ze základního pořadí druhý řádek permutace $P$.

Např. použijeme-li postupně transpozice $(1,2), (1,3)$ a $(1,5)$, budeme postupně dostávat pořadí $(1,2,3,4,5), (2,1,3,4,5), (2,3,1,4,5)$ a $(2,3,5,4,1)$, a tedy $P = (1,2)\circ(1,3)\circ(1,5)$.

Podobně také dostaneme $P = (1,2) \circ (1,3) \circ (1,4) \circ (1,5) \circ (4,5)$.

Vidíme proto, že i když bylo předem zřejmé, že permutace $P$ se rozloží na lichý počet transpozic, pak tento počet není určen jednoznačně.

**Věta 5.9** *Vznikne-li pořadí $\pi'$ z pořadí $\pi$ pomocí permutace $P$, pak $sgn\ \pi' = sgn\ P \cdot sgn\ \pi$.*

D ů k a z: Předpokládejme, že uvažujeme pořadí na $n$-prvkové množině. Uvažujme posloupnost všech $n!$ pořadí, které začíná pořadím $\pi$ a které má stejnou vlastnost jako posloupnost pořadí ve větě 5.6. Má-li $\pi'$ stejné znaménko jako $\pi$, pak $\pi'$ musí v této posloupnosti ležet na lichém místě. Tzn., že složíme-li odpovídající sudý počet transpozic, pomocí kterých jsme se postupně dostali od $\pi$ k $\pi'$, dostaneme sudou permutaci $P$, pro níž ovšem platí, že právě pomocí ní vzniklo $\pi'$ z $\pi$. Analogicky pro případ $sgn\ \pi' = -sgn\ \pi$. □

(Na základě této věty jsme si ověřili skutečnost, že každá transpozice je lichá.)

**Věta 5.10** *Nechť $\pi_1, \pi_2, \ldots, \pi_{n!}$ je libovolná posloupnost všech pořadí $n$-prvkové množiny. (Každé pořadí se v ní vyskytuje právě jednou.) Nechť $P$ je libovolná permutace. Označíme-li $\pi'_i$ pořadí, které vznikne z pořadí $\pi_i$, pomocí permutace $P$ $(i = 1, 2, \ldots, n!)$, pak je opět $\pi'_1, \pi'_2, \ldots, \pi'_{n!}$ posloupnost všech pořadí dané $n$-prvkové množiny.*

D ů k a z: Označme $\pi_0$ základní pořadí a pomocí posloupnosti pořadí $\pi_1, \pi_2, \ldots, \pi_{n!}$ posloupnost permutací $P_1, P_2, \ldots, P_{n!}$ takovou, že

$$P_i = \begin{pmatrix} \pi_0 \\ \pi_i \end{pmatrix}, i = 1, 2, \ldots, n!.$$

Je zřejmé, že platí

$$P_i \circ P = \begin{pmatrix} \pi_0 \\ \pi'_i \end{pmatrix}.$$

Předpokládejme, že se v posloupnosti $\pi'_1, \pi'_2, \ldots, \pi'_{n!}$ vyskytnou dvě pořadí $\pi'_i, \pi'_j$ taková, že $i \neq j$ a $\pi'_i = \pi'_j$. To ovšem znamená, že

$$P_i \circ P = \begin{pmatrix} \pi_0 \\ \pi'_i \end{pmatrix} = \begin{pmatrix} \pi_0 \\ \pi'_j \end{pmatrix} = P_j \circ P,$$

tedy $P_i \circ P = P_j \circ P$. Odtud dostáváme $(P_i \circ P) \circ P^{-1} = (P_j \circ P) \circ P^{-1}$ a z asociativnosti skládání permutací také $P_i \circ (P \circ P^{-1}) = P_j \circ (P \circ P^{-1})$. Protože $P \circ P^{-1}$ je identická permutace $P_0$, musí platit $P_i = P_j$.

Avšak $P_i = \begin{pmatrix} \pi_0 \\ \pi_i \end{pmatrix}$, $P_j = \begin{pmatrix} \pi_0 \\ \pi_j \end{pmatrix}$, a proto také $\pi_i = \pi_j$.

V posloupnosti $\pi_1, \pi_2, \ldots, \pi_{n!}$ ovšem platí, že pro $i \neq j$ nastane $\pi_i \neq \pi_j$, to je spor. Proto v posloupnosti

$$\pi'_1, \pi'_2, \ldots, \pi'_{n!}$$

jsou všechna pořadí navzájem různá. □

## 5.2 Základní vlastnosti determinantů

V této části se budeme zabývat čtvercovými maticemi nad libovolným číselným tělesem $\mathcal{T}$. Každé takové matici přiřadíme číslo z tělesa $\mathcal{T}$ nazývané determinant matice. Jak v definici, tak i při studiu základních vlastností determinantů budeme používat výsledků týkajících se permutací.

**Definice 5.8** *Nechť*

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

*je čtvercová matice stupně $n$ nad číselným tělesem $\mathcal{T}$.*

Determinantem matice $A$ *pak rozumíme číslo* $\det A$ *z tělesa $\mathcal{T}$ takové, že*

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

*kde sčítáme přes všechny permutace*

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

*množiny $\{1, 2, \ldots, n\}$. Každý ze součinů*

$$a_{1k_1} \cdot a_{2k_2} \cdot \ldots \cdot a_{nk_n}$$

*nazýváme* člen determinantu $\det A$.

`Poznámka:`

a) Uvědomme si, že permutace je bijekcí množiny na sebe. Proto determinant matice $A$ můžeme také popsat slovy takto: Je to prvek z $\mathcal{T}$, který je součtem $n!$ takových součinů o $n$ prvcích matice $A$, ve kterých je z každého řádku a z každého sloupce matice $A$ právě jeden prvek, přičemž každý ze součinů je vynásoben znaménkem permutace určené řádkovými a sloupcovými indexy prvků tohoto součinu.

b) Pro označení čísla $\det A$ budeme také používat označení $|A|$, popř.

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

**Příklad 5.9**

a) Určeme determinant matice 2. stupně

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

Jako členy determinantu $\det A$ budou vystupovat součiny $a_{11}a_{22}$ a $a_{12}a_{21}$. Určíme jejich znaménka. Pro první z nich je to

$$sgn \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = 1$$

a pro druhý

$$sgn \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = -1.$$

Tedy $\det A = a_{11}a_{22} - a_{12}a_{21}$.

b) Podobně určíme determinant matice 3. stupně

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

Definici členu determinantu vyhovují součiny $a_{11}a_{22}a_{33}$, $a_{12}a_{23}a_{31}$, $a_{21}a_{32}a_{13}$, $a_{13}a_{22}a_{31}$, $a_{12}a_{21}a_{33}$, $a_{23}a_{32}a_{11}$. Snadno určíme znaménka permutací sestavených z sloupcových a řádkových indexů těchto členů, která současně určují, s jakým znaménkem budou členy v determinantu vystupovat. Zjistíme, že první tři členy budou mít znaménko „$+$“ a zbývající znaménko „$-$“. Platí tedy

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

$$-a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{23}a_{32}a_{11}.$$

`Poznámka`: Uvedená vyjádření determinantů současně ukazují obecnou metodou, jak vypočíst konkrétní determinanty 2. a 3. stupně. Tato metoda se také nazývá *Sarrusovo pravidlo*. Ale pozor: Sarrusovo pravidlo nemá tak přehlednou analogii pro determinanty matic stupňů vyšších než tři.

**Příklad 5.10** Určete determinanty

$$\begin{vmatrix} 3 & 5 \\ 4 & 7 \end{vmatrix}, \begin{vmatrix} -2 & 1 & 4 \\ 5 & 2 & -1 \\ 3 & 1 & 6 \end{vmatrix}.$$

Podle předchozího příkladu platí

$$\begin{vmatrix} 3 & 5 \\ 4 & 7 \end{vmatrix} = 21 - 20 = 1.$$

Analogicky $\begin{vmatrix} -2 & 1 & 4 \\ 5 & 2 & -1 \\ 3 & 1 & 6 \end{vmatrix} = -24 - 3 + 20 - 24 - 2 - 30 = -63.$

**Definice 5.9** *Je-li $A = ||a_{ij}||$ matice typu $m \times n$, potom* maticí transponovanou k matici *$A$ nazýváme matici $A^T = ||a_{ij}||$ typu $n \times m$, která vznikne z matice $A$ vzájemnou záměnou řádků a sloupců (tj. překlopením matice $A$ podle hlavní diagonály).*

`Poznámka`: V dalším textu budeme bez dalšího komentáře používat některých zřejmých vlastností operace transponování matic, zejména

$$(A + B)^T = A^T + B^T,$$

$$(cA)^T = cA^T,$$

$$(AC)^T = C^T A^T,$$

kde $A, B \in M_{m\times n}(\mathcal{T})$, $C \in M_{n\times p}(\mathcal{T})$, $c \in \mathcal{T}$. (Čtenář si může sám ověřit platnost uvedených rovností.)

**Věta 5.11** *Pro každou čtvercovou matici $A \in M_n(\mathcal{T})$ platí*

$$\det A^T = \det A.$$

D ů k a z: Nechť $A = ||a_{ij}|| \in M_n(\mathcal{T})$. Označíme-li $A^T = ||b_{ij}||$, pak platí $b_{ij} = a_{ji}$, $i = 1, 2, \dots, n$, $j = 1, 2, \dots, n$. Podle definice determinantu platí

$$\det A = \sum_P sgn\ P\ a_{1k_1} a_{2k_2} \dots a_{nk_n} = \sum_P sgn\ P\ b_{k_1 1} b_{k_2 2} \dots b_{k_n n},$$

kde sčítáme přes všechny permutace $P = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$ na $\{1, 2, \dots, n\}$. Ovšem proběhne-li $P = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$ všechny permutace na $\{1, 2, \dots, n\}$, potom $P' = \begin{pmatrix} k_1 & k_2 & \dots & k_n \\ 1 & 2 & \dots & n \end{pmatrix}$ proběhne také všechny permutace na $\{1, 2, \dots, n\}$ a platí $sgn\ P' = sgn\ P^{-1} = sgn\ P$. Platí tedy

$$\sum_P sgn\ P\ b_{k_1 1} b_{k_2 2} \dots b_{k_n n} = \sum_{P'} sgn\ P'\ b_{1k_1} b_{2k_2} \dots b_{nk_n} = \det A^T.$$

Proto $\det A^T = \det A$. □

`Poznámka:` Věta 5.11 má velký význam pro práci s determinanty. Budeme-li totiž provádět úvahy týkající se sloupců matic, potom tyto úvahy jsou vlastně také úvahami týkajícími se řádků transponovaných matic.

Takže dokážeme-li některá tvrzení o determinantech *všech* matic taková, že v jejich formulaci se používají řádky matic, potom platí analogické tvrzení, ve kterých se používají sloupce matic.

**Věta 5.12** *Má-li čtvercová matice $A$ v některém řádku samé nuly, pak* $\det A = 0$.

D ů k a z: Nechť $A \in M_n(\mathcal{T})$ je matice, která má v $i$-tém řádku samé nuly. Protože podle definice determinantu se v každém členu determinantu vyskytuje právě jeden prvek z $i$-tého řádku, musí být každý člen determinantu roven nule, a proto je i celý determinant roven nule. □

**Věta 5.13** *Má-li matice $A \in M_n(\mathcal{T})$ všechny prvky pod hlavní diagonálou rovny nule, potom* $\det A$ *je roven součinu $a_{11}a_{22}\dots a_{nn}$ prvků na hlavní diagonále.*

D ů k a z: Je zřejmé, že součin prvků na hlavní diagonále je členem determinantu, který vystupuje s kladným znaménkem. (Řádkové a sloupcové indexy zde tvoří identickou permutaci.) Je-li $a_{1k_1}a_{2k_2}\dots a_{nk_n}$ další člen determinantu, potom alespoň pro jeden index $i$ $(i = 1, 2, \dots, n)$ musí platit $k_i < i$. Pokud by totiž pro všechny indexy $j$ $(j = 1, 2, \dots, n)$ platilo $k_j \geq j$, potom by

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

nebyla bijekce. Proto alespoň jeden prvek ze součinu $a_{1k_1}a_{2k_2}\dots a_{nk_n}$ různého od součinu $a_{11}a_{22}\dots a_{nn}$ je roven nule, a tedy i každý takový součin je nulový. To ovšem znamená, že $\det A = a_{11}a_{22}\dots a_{nn}$. □

**Věta 5.14** *Vznikne-li matice $B$ ze čtvercové matice $A$ stupně $n$ záměnou $i$-tého a $j$-tého řádku, kde $i \neq j$, potom* $\det B = -\det A$.

D ů k a z: Předpokládejme, že $i < j$, a uvažujme transpozici $T = (i, j)$. Jestliže

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

je permutace z $S_n = S(\{1, 2, \dots, n\})$, potom

$$P' = T \circ P = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ k_1 & \dots & k_j & \dots & k_i & \dots & k_n \end{pmatrix}$$

je opět permutace z $S_n$ a podle věty 5.9 platí, že proběhne-li $P$ všechny permutace z $S_n$, proběhne $P'$ také všechny permutace z $S_n$. Přitom podle věty 5.4 platí, že $sgn\ P' = -sgn\ P$. Proto dostáváme

$$\det B = \sum_P sgn\ P\ b_{1k_1} b_{2k_2} \dots b_{ik_i} \dots b_{jk_j} \dots b_{nk_n} =$$

$$= \sum_P sgn\ P\ a_{1k_1} \dots a_{ik_j} \dots a_{jk_i} \dots a_{nk_n} =$$

$$= \sum_{P'} sgn\ P'\ a_{1k_1} \dots a_{ik_i} \dots a_{jk_j} \dots a_{nk_n} = -\det A.$$

□

**Věta 5.15** *Vznikne-li matice $B$ z matice $A \in M_n(\mathcal{T})$ provedením některé permutace $P$ na řádky matice $A$, potom*

$$\det B = sgn\ P \cdot \det A.$$

D ů k a z: Tvrzení je důsledkem věty 5.14 a věty 5.9. □

**Věta 5.16** *Jestliže se v matici $A \in M_n(\mathcal{T})$ rovnají $i$-tý a $j$-tý řádek ($i \neq j$), pak* $\det A = 0$.

D ů k a z: Zaměníme-li $i$-tý a $j$-tý řádek v matici $A$, dostaneme opět matici $A$, ovšem podle věty 5.14 pak platí $\det A = -\det A$. Tedy $\det A = 0$. □

**Definice 5.10**

a) *Nechť $A = ||a_{ij}||$ je matice typu $m \times n$. Potom každou matici, která vznikne z matice $A$ vynecháním některých řádků a některých sloupců, nazýváme* dílčí maticí matice $A$.

b) *Je-li dílčí matice matice $A$ čtvercová, potom její determinant nazýváme* subdeterminantem matice $A$.

**Definice 5.11**

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

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

**Příklad 5.11** Určeme algebraické doplňky $\mathcal{A}_{12}$ a $\mathcal{A}_{33}$ prvků matice

$$A = \begin{pmatrix} 2 & 5 & 1 \\ 0 & -6 & 2 \\ 5 & 1 & -3 \end{pmatrix}.$$

Platí $\mathcal{M}_{12} = \begin{vmatrix} 0 & 2 \\ 5 & -3 \end{vmatrix} = -10$, $\mathcal{M}_{33} = \begin{vmatrix} 2 & 5 \\ 0 & -6 \end{vmatrix} = -12$, tedy $\mathcal{A}_{12} = (-1)^{1+2}(-10) = 10$, $\mathcal{A}_{33} = (-1)^{3+3}(-12) = -12$.

`Poznámka:`

a) Nechť $\overrightarrow{a_1}, \dots, \overrightarrow{a_n}$ jsou řádkové vektory a $\overrightarrow{b_1}^T, \dots, \overrightarrow{b_n}^T$ sloupcové vektory matice $A \in M_n(\mathcal{T})$. Potom budeme také zkráceně zapisovat

$$A = ||\overrightarrow{b_1}^T, \dots, \overrightarrow{b_n}^T||, \det A = |\overrightarrow{b_1}^T, \dots, \overrightarrow{b_n}^T|$$

a

$$A = \left\|\begin{vmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix}\right\|, \det A = \begin{vmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix}.$$

b) Jsou-li $i, j \in \{1, \dots, n\}$, pak označíme

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

**Věta 5.17 (Laplaceova)** *Nechť $A = ||a_{ik}|| \in M_n(\mathcal{T})$. Potom*

*a) pro každé $i = 1, \dots, n$ platí*

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

*b) pro každé $i, j = 1, \dots, n$, $i \neq j$ platí*

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

`Poznámka`: Laplaceova větu můžeme stručně zapsat takto: Jestliže $i, j = 1, \dots, n$, potom platí

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

D ů k a z (věty 5.17): Víme že

$$\det A = \sum_{P} sgn\ P \cdot a_{1k_1} \dots a_{nk_n},$$

kde $P$ je libovolná permutace z $S_n = S(\{1, 2, \dots, n\})$. Tedy každý člen determinantu matice $A$ obsahuje právě jeden prvek z $i$-tého řádku ($i = 1, \dots, n$), proto můžeme psát

$$\det A = \begin{vmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix} = \sum_{k=1}^{n} a_{ik}\mathcal{B}_{ik},$$

kde $\mathcal{B}_{ik}$ je prvek z $\mathcal{T}$.

Pokud zaměníme v matici $A$ $j$-tý řádek $i$-tým řádkem (např. $i < j$), platí podle věty 5.16

$$0 = \begin{vmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{a_i} \\ \vdots \\ \overrightarrow{a_i} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix} = \sum_{k=1}^{n} a_{ik}\mathcal{B}_{jk}.$$

Abychom dokázali tvrzení, stačí dokázat, že $\mathcal{B}_{ik} = \mathcal{A}_{ik}$ pro každá $i, k = 1, 2, \dots, n$.

a) Nejdříve dokážeme, že $\mathcal{B}_{11} = \mathcal{A}_{11}$. Je zřejmé, že součet všech členů determinantu matice $A$ obsahujících $a_{11}$ můžeme zapsat ve tvaru

$$a_{11}\mathcal{B}_{11} = \sum_{P} sgn\ P\ a_{11}a_{2k_2} \dots a_{nk_n},$$

kde sčítáme přes všechny permutace

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

To tedy znamená, že

$$\mathcal{B}_{11} = \sum_{P'} sgn\ P'\ a_{2k_2}a_{3k_3} \dots a_{nk_n},$$

kde $P'$ je libovolná permutace množiny $\{2, 3, \ldots, n\}$ ve tvaru

$$P = \begin{pmatrix} 2 & 3 & \ldots & n \\ k_2 & k_3 & \ldots & k_n \end{pmatrix}.$$

Protože platí $sgn\ P = sgn\ P'$, je $\mathcal{B}_{11} = \mathcal{M}_{11}$, a protože $\mathcal{A}_{11} = (-1)^2\mathcal{M}_{11}$, platí také $\mathcal{B}_{11} = \mathcal{A}_{11}$.

b) Nyní dokážeme obecně, že $\mathcal{B}_{ij} = \mathcal{A}_{ij}$ pro každé $i, j = 1, \ldots, n$. Proveďme nejdříve permutaci

$$P_1 = \begin{pmatrix} 1 & 2 & \ldots & i-1 & i & i+1 & \ldots & n \\ i & 1 & \ldots & i-2 & i-1 & i+1 & \ldots & n \end{pmatrix}$$

na řádky a potom permutaci

$$P_2 = \begin{pmatrix} 1 & 2 & \ldots & j-1 & j & j+1 & \ldots & n \\ j & 1 & \ldots & j-2 & j-1 & j+1 & \ldots & n \end{pmatrix}$$

na sloupce matice $A$.
Ve výsledku dostaneme matici

$$\mathcal{C} = ||c_{ik}|| = \left\| \begin{matrix} a_{ij} & a_{i1} & \cdots & a_{i,j-1} & a_{i,j+1} & \cdots & a_{in} \\ a_{1j} & a_{11} & \cdots & a_{1,j-1} & a_{1,j+1} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{i-1,j} & a_{i-1,1} & \cdots & a_{i-1,j-1} & a_{i-1,j+1} & \cdots & a_{i-1,n} \\ a_{i+1,j} & a_{i+1,1} & \cdots & a_{i+1,j-1} & a_{i+1,j+1} & \cdots & a_{i+1,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{nj} & a_{n1} & \cdots & a_{n,j-1} & a_{n,j+1} & \cdots & a_{nn} \end{matrix} \right\|.$$

Protože je podle věty 5.8 $sgn\ P_1 = (-1)^{i-1}$ a $sgn\ P_2 = (-1)^{j-1}$, platí podle vět 5.15 a 5.11, že

$$\det C = (-1)^{i-1}(-1)^{j-1}\det A = (-1)^{i+j}\det A.$$

Označme (analogicky jako pro matici $A$) symbolem $\mathcal{C}_{ik}$ minor matice $C$ příslušný k prvku $c_{ik}$ a $\mathcal{D}_{ik}$ prvek z $\mathcal{T}$ vzniklý sečtením členů $\det C$ obsahujících $c_{ik}$ uvažovaných se znaménky po vytknutí prvku $c_{ik}$ $(i, k = 1, \ldots, n)$. Platí $c_{11} = a_{ik}$, $\mathcal{C}_{11} = \mathcal{M}_{ik}$ a

$$\det C = \sum_{k=1}^{n} c_{ik}\mathcal{D}_{ik}, \quad i = 1, \ldots, n.$$

Podle části a) důkazu přitom platí $\mathcal{D}_{11} = \mathcal{C}_{11}$. Proto dostáváme
$a_{i1}\mathcal{B}_{i1} + \ldots + a_{ij}\mathcal{B}_{ij} + \ldots + a_{in}\mathcal{B}_{in} = \det A = (-1)^{i+j}\det C = (-1)^{i+j}(c_{11}\mathcal{D}_{11} + \ldots + c_{1n}\mathcal{D}_{1n}) = (-1)^{i+j}(a_{ij}\mathcal{M}_{ij} + a_{i1}\mathcal{D}_{12} + \ldots + a_{i,j-1}\mathcal{D}_{ij} + a_{i,j+1}\mathcal{D}_{i,j+i} + \ldots + a_{in}\mathcal{D}_{in})$,
a přitom $\mathcal{D}_{1k} = (-1)^{i+j}\mathcal{B}_{i,k-1}$, $k = 2, \ldots, j$, $\mathcal{D}_{1l} = (-1)^{i+j}\mathcal{B}_{il}$, $l = j+1, \ldots, n$. Platí proto

$$\mathcal{B}_{ij} = (-1)^{i+j}\mathcal{M}_{ij} = \mathcal{A}_{ij}.$$

□

**Věta 5.18** *Vznikne-li matice $B$ vynásobením $i$-tého řádku matice $A \in M_n(\mathcal{T})$ prvkem $c \in \mathcal{T}$, potom platí*

$$\det B = c \cdot \det A.$$

D ů k a z: Nechť $i = 1, \ldots, n$, $A = \left\| \begin{matrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{a_i} \\ \vdots \\ \overrightarrow{a_n} \end{matrix} \right\|$ a $B = \left\| \begin{matrix} & \overrightarrow{a_1} \\ & \vdots \\ c\cdot & \overrightarrow{a_i} \\ & \vdots \\ & \overrightarrow{a_n} \end{matrix} \right\|$ Potom podle Laplaceovy věty platí

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

□

**Důsledek:** Jestliže $A \in M_n(\mathcal{T})$, $c \in \mathcal{T}$, potom

$$\det(cA) = c^n \det A.$$

□

**Věta 5.19** *Jestliže $A \in M_n(\mathcal{T})$, a platí-li, že $i$-tý řádek $\overrightarrow{a_i}$ matice $A$ je roven součtu vektorů $\overrightarrow{b}$ a $\overrightarrow{c}$, potom*

$$\begin{vmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{a_i} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix} = \begin{vmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{b} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix} + \begin{vmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{c} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix}.$$

D ů k a z: Nechť $\overrightarrow{a_i} = (a_{i1}, a_{i2}, \ldots, a_{in})$, $\overrightarrow{b} = (b_1, b_2, \ldots, b_n)$, $\overrightarrow{c} = (c_1, c_2, \ldots, c_n)$. Potom platí

$$\begin{vmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{a_i} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix} = \sum_{k=1}^{n} a_{ik} \mathcal{A}_{ik} = \sum_{k=1}^{n} (b_k + c_k) \mathcal{A}_{ik} = \sum_{k=1}^{n} b_k \mathcal{A}_{ik} + \sum_{k=1}^{n} c_k \mathcal{A}_{ik} = \begin{vmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{b} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix} + \begin{vmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{c} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix}.$$

□

**Věta 5.20** *Nechť $A \in M_n(\mathcal{T})$. Vznikne-li matice $B \in M_n(\mathcal{T})$ z matice $A$ tak, že k některému řádku matice $A$ přičteme libovolnou lineární kombinaci ostatních řádků této matice, pak platí*

$$\det B = \det A.$$

D ů k a z: Bez újmy na obecnosti můžeme předpokládat, že k prvnímu řádku $\overrightarrow{a_1}$ matice $A$ přičteme lineární kombinaci

$$\overrightarrow{b} = \sum_{i=2}^{n} c_i \overrightarrow{a_i}$$

ostatních řádků. (Jinak bychom mohli podle věty 5.15 řádky v obou maticích současně zaměnit.) Pak ale platí

$$\begin{vmatrix} \overrightarrow{a_1} + \overrightarrow{b} \\ \overrightarrow{a_2} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix} = \begin{vmatrix} \overrightarrow{a_1} \\ \overrightarrow{a_2} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix} + c_2 \begin{vmatrix} \overrightarrow{a_2} \\ \overrightarrow{a_2} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix} + \cdots + \begin{vmatrix} \overrightarrow{a_n} \\ \overrightarrow{a_2} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix}.$$

Na pravé straně této rovnosti dostáváme součet determinantů, které jsou (s eventuální výjimkou prvního) determinanty matic, ve kterých se rovnají dva různé řádky. Podle věty 5.16 jsou takové determinanty rovny 0, a proto platí

$$\begin{vmatrix} \overrightarrow{a_1} + \overrightarrow{b} \\ \overrightarrow{a_2} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix} = \begin{vmatrix} \overrightarrow{a_1} \\ \overrightarrow{a_2} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix} = \det A.$$

□

**Věta 5.21** *Jsou-li řádkové vektory matice $A \in M_n(\mathcal{T})$ lineárně závislé, potom*

$$\det A = 0.$$

D ů k a z: Předpokládejme, že řádkové vektory matice $A$ jsou lineárně závislé. Pak je ale jeden z nich lineární kombinací ostatních, např. platí (bez újmy na obecnosti)

$$\overrightarrow{a_1} = \sum_{i=2}^{n} c_i \overrightarrow{a_i}.$$

Potom podle vět 5.18, 5.18 a 5.16 dostáváme

$$\det A = \begin{vmatrix} \overrightarrow{a_1} \\ \overrightarrow{a_2} \\ \overrightarrow{a_3} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix} = c_2 \begin{vmatrix} \overrightarrow{a_2} \\ \overrightarrow{a_2} \\ \overrightarrow{a_3} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix} + c_3 \begin{vmatrix} \overrightarrow{a_3} \\ \overrightarrow{a_2} \\ \overrightarrow{a_3} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix} + \cdots + c_n \begin{vmatrix} \overrightarrow{a_n} \\ \overrightarrow{a_2} \\ \overrightarrow{a_3} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix} = 0.$$

□

Předchozích vět budeme využívat k praktickému výpočtu determinantů matic vyšších stupňů. Podle Laplaceovy věty můžeme výpočet determinantů matic $n$-tého stupně převést vždy na výpočet $n$ determinantů $(n-1)$-ho stupně. Přitom každý z těchto determinantů $(n-1)$-ho stupně je vynásoben (kromě znaménka) prvkem určitého řádku (nebo sloupce) dané matice.

Proto převedeme-li danou matici na takovou matici, která má stejný determinant jako původní matice, ale má v řádku některé prvky rovny 0, nemusíme při rozvoji podle Laplaceovy věty počítat v nové matici algebraické doplňky nulových prvků používaného řádku. V některých případech můžeme dokonce dosáhnou toho, že v jistém řádku (nebo sloupci) budou rovny nule všechny prvky s výjimkou jednoho. Pak můžeme převést výpočet determinantu matice $n$-tého stupně na výpočet jednoho determinantu $(n-1)$ stupně. V každém případě ale můžeme u konkrétních matic postupně snižovat stupeň tak dlouho, dokud nedosáhneme matice třetího nebo druhého stupně, a pak použít Sarrusovo pravidlo.

**Příklad 5.12** Vypočítejte determinant

$$a)\begin{vmatrix} -2 & 3 & -1 & 2 \\ 1 & -2 & 0 & 4 \\ 2 & -4 & -2 & 5 \\ -3 & 2 & 1 & -5 \end{vmatrix} \qquad b)\begin{vmatrix} x & y & 0 & 0 & \cdots & 0 & 0 \\ 0 & x & y & 0 & \cdots & 0 & 0 \\ 0 & 0 & x & y & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & x & y \\ y & 0 & 0 & 0 & \cdots & 0 & x \end{vmatrix}$$

kde v b) je determinant matice $n$-tého stupně.

$$\text{a)}\begin{vmatrix} -2 & 3 & -1 & 2 \\ 1 & -2 & 0 & 4 \\ 2 & -4 & -2 & 5 \\ -3 & 2 & 1 & -5 \end{vmatrix} = \begin{vmatrix} 0 & -1 & -1 & 10 \\ 1 & -2 & 0 & 4 \\ 0 & 0 & -2 & -3 \\ 0 & -4 & 1 & 7 \end{vmatrix} = 1\cdot(-1)^{2+1}\cdot\begin{vmatrix} -1 & -1 & 10 \\ 0 & 2 & -3 \\ -4 & 1 & 7 \end{vmatrix} =$$

$$= (-1)\begin{vmatrix} -1 & 0 & 0 \\ 0 & -2 & -3 \\ -4 & 5 & -33 \end{vmatrix} = (-1)(-1)(-1)^{1+1}\begin{vmatrix} -2 & -3 \\ 5 & -33 \end{vmatrix} = 66+15 = 81$$

$$\text{b)}\begin{vmatrix} x & y & 0 & 0 & \cdots & 0 & 0 \\ 0 & x & y & 0 & \cdots & 0 & 0 \\ 0 & 0 & x & y & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & x & y \\ y & 0 & 0 & 0 & \cdots & 0 & x \end{vmatrix} = x\cdot(-1)^{1+1}\begin{vmatrix} x & y & 0 & \cdots & 0 & 0 \\ 0 & x & y & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & x & y \\ 0 & 0 & 0 & \cdots & 0 & x \end{vmatrix} +$$

$$+y\cdot(-1)^{n+1}\begin{vmatrix} y & 0 & 0 & \cdots & 0 & 0 \\ x & y & 0 & \cdots & 0 & 0 \\ 0 & x & y & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & x & y \end{vmatrix} = x\cdot x^{n-1} + (-1)^{n+1}\cdot y\cdot y^{n-1} = x^n + (-1)^{n+1}\cdot y^n.$$

## 5.3 Determinant součinu matic

Hlavním obsahem této části je důkaz tvrzení o tom, jak spočítat determinant součinu dvou čtvercových matic téhož stupně. Toto tvrzení bude mít zásadní význam např. při studiu vlastností množiny tzv. regulárních matic.

**Věta 5.22** *Nechť $A = ||a_{ij}|| \in M_n(\mathcal{T})$, $n > 1$, je taková matice, že platí*

$$A = \begin{Vmatrix} B & D \\ N_{s\times r} & C \end{Vmatrix},$$

*kde $B$ je čtvercová matice stupně $r$ a $C$ je čtvercová matice stupně $s$. (Samozřejmě $r + s = n$.) Potom platí*

$$\det A = \det B \cdot \det C.$$

D ů k a z: Provedeme indukcí podle stupně matice $A$.

a) Je-li $A \in M_n(\mathcal{T})$, pak $A$ je tvaru

$$A = \begin{Vmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{Vmatrix},$$

a platí $\det A = a_{11}a_{22}$.

b) Nechť tvrzení platí pro všechny matice typu nejvýše $n-1$ ($n > 2$). Uvažujme matici $n$-tého stupně, pro kterou platí

$$A = \begin{Vmatrix} B & D \\ N_{s\times r} & C \end{Vmatrix},$$

kde $B \in M_r(\mathcal{T})$, $C \in M_s(\mathcal{T})$.
Podle Laplaceovy věty pak platí

$$\det A = \sum_{j=1}^{n} a_{1j}\mathcal{A}_{1j} = \sum_{j=1}^{n} (-1)^{1+j} a_{1j}\mathcal{M}_{1j}.$$

Přitom $\mathcal{M}_{1j} = \det M_{1j}$, kde matice $M_{1j}$ vznikne z $A$ vynecháním prvního řádku a $j$-tého sloupce. Ovšem každá z matic $M_{1j}$ ($j = 1, \ldots, n$) je stupně $n-1$ a přitom typu, který je uvažován ve větě, proto na ni můžeme použít indukční předpoklad.
Označme $B_{1j}$ matici, která vznikne z matice $B$ vynecháním prvního řádku a $j$-tého sloupce ($j = 1, \ldots, r$). Pak platí

$$\mathcal{M}_{1j} = \det M_{1j} = \det B_{1j} \cdot \det C \ (j = 1, \ldots, r).$$

Ovšem matice $M_{1,r+1}, \ldots, M_{1,n}$ můžeme rozložit na takový tvar, že levá horní čtvercová matice je stupně $r$-tého, a tedy má v posledním řádku samé nuly. Determinant každé z těchto matic je ovšem také roven nule, proto podle indukčního předpokladu platí také

$$\det M_{1,r+k} = 0 \ (k = 1, \ldots, s).$$

Takže platí

$$\det A = \sum_{j=1}^{r}(-1)^{1+j}a_{ij}\det B_{ij}\det C = \left(\sum_{j=1}^{n}(-1)^{1+j}a_{1j}\det B_{1j}\right)\det C = \det B \cdot \det C.$$

□

**Věta 5.23** *Nechť $A$ a $B$ jsou čtvercové matice stupně $n$-tého nad číselným tělesem $\mathcal{T}$. Pak platí*

$$\det A \cdot B = \det A \cdot \det B,$$

*tj.* $|AB| = |A| \cdot |B|$.

D ů k a z: Nechť $A = ||a_{ij}||$, $B = ||b_{ij}|| \in M_n(\mathcal{T})$. Uvažujme čtvercovou matici $U$ $2n$-tého stupně takovou, že

$$A = \left\|\begin{array}{rrcrrrcr} a_{11} & a_{12} & \cdots & a_{1n} & 0 & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2n} & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} & 0 & 0 & \cdots & 0 \\ -1 & 0 & \cdots & 0 & b_{11} & b_{12} & \cdots & b_{1n} \\ 0 & -1 & \cdots & 0 & b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 & b_{n1} & b_{n2} & \cdots & b_{nn} \end{array}\right\|,$$

Vzhledem k tomu,že determinant matice transponované je roven determinantu původní matice a vzhledem k větě 5.22, platí potom

$$\det U = \det A \cdot \det B.$$

K prvnímu řádku matice $U$ přičteme nyní lineární kombinaci řádků $(n+1)$-ho, …, $2n$-tého s koeficienty $a_{11}$, $a_{12}$, …, $a_{1n}$.

Analogicky přičteme k druhému řádku lineární kombinaci týchž řádků s koeficienty $a_{21}$, $a_{22}$, …, $a_{2n}$, atd., až k $n$-tému řádku přičteme lineární kombinaci opět týchž řádků s koeficienty $a_{n1}$, $a_{n2}$, …, $a_{nn}$.

Podle věty 5.20 a vět 5.14 a 5.11 potom platí

$$\det A \cdot \det B =$$

$$= \begin{vmatrix} 0 & 0 & \cdots & 0 & \sum_{j=1}^{n} a_{1j}b_{j1} & \sum_{j=1}^{n} a_{1j}b_{j2} & \cdots & \sum_{j=1}^{n} a_{1j}b_{jn} \\ 0 & 0 & \cdots & 0 & \sum_{j=1}^{n} a_{2j}b_{j1} & \sum_{j=1}^{n} a_{2j}b_{j2} & \cdots & \sum_{j=1}^{n} a_{2j}b_{jn} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \sum_{j=1}^{n} a_{nj}b_{j1} & \sum_{j=1}^{n} a_{nj}b_{j2} & \cdots & \sum_{j=1}^{n} a_{nj}b_{jn} \\ -1 & 0 & \cdots & 0 & b_{11} & b_{12} & \cdots & b_{1n} \\ 0 & -1 & \cdots & 0 & b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 & b_{n1} & b_{n2} & \cdots & b_{nn} \end{vmatrix} = \begin{vmatrix} N & AB \\ -E & B \end{vmatrix}.$$

Zaměníme-li nyní první sloupec matice s $(n+1)$-ním sloupcem, druhý sloupec s $(n+2)$-hým sloupcem, atd., až $n$-tý sloupec s $2n$-tým sloupcem, dostaneme matici, pro kterou platí

$$\det A \cdot \det B =$$

$$= (-1)^n \begin{vmatrix} \sum_{j=1}^{n} a_{1j}b_{j1} & \sum_{j=1}^{n} a_{1j}b_{j2} & \cdots & \sum_{j=1}^{n} a_{1j}b_{jn} & 0 & 0 & \cdots & 0 \\ \sum_{j=1}^{n} a_{2j}b_{j1} & \sum_{j=1}^{n} a_{2j}b_{j2} & \cdots & \sum_{j=1}^{n} a_{2j}b_{jn} & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \sum_{j=1}^{n} a_{nj}b_{j1} & \sum_{j=1}^{n} a_{nj}b_{j2} & \cdots & \sum_{j=1}^{n} a_{nj}b_{jn} & 0 & 0 & \cdots & 0 \\ b_{11} & b_{12} & \cdots & b_{1n} & -1 & 0 & \cdots & 0 \\ b_{21} & b_{22} & \cdots & b_{2n} & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} & 0 & 0 & \cdots & -1 \end{vmatrix}.$$

Podle věty 5.22 tedy dostáváme

$$\det A \cdot \det B = (-1)^n \begin{vmatrix} AB & N \\ B & -E \end{vmatrix} =$$

$$= (-1)^n \det AB \cdot \det(-E) = (-1)^n \det AB \cdot (-1)^n = \det AB.$$

□

## 5.4 Cvičení

**5.1** Určete znaménko pořadí (permutace)

a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 5 & 1 & 6 & 2 & 3 \end{pmatrix}$; b) $\begin{pmatrix} 2 & 1 & 4 & 5 & 3 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$;

c) $(1, 9, 6, 3, 2, 5, 4, 7, 8)$;

d) $(1, 3, 5, \ldots, 2n-1, 2, 4, 6, \ldots, 2n)$;

e) $(2, 4, 6, \ldots, 2n, 1, 3, 5, \ldots, 2n-1)$;

f) $(2, 5, 8, \ldots, 3n-1, 3, 6, 9, \ldots, 3n, 1, 4, 7, \ldots, 3n-2)$;

g) $(2, 5, 8, \ldots, 3n-1, 1, 4, 7, \ldots, 3n-2, 3, 6, 9, \ldots, 3n)$.

[ a)-; b)+; c)-; d)$(-1)^{\frac{n(n-1)}{2}}$; e)$(-1)^{\frac{n(n+1)}{2}}$; f) $(-1)^{\frac{n(3n+1)}{2}}$; g) $(-1)^{\frac{n(3n-1)}{2}}$ ]

**5.2** Vypočítejte permutaci

a) $A^2$ b) $B^3$ c) $C^{100}$ d) $X$ z rovnice $DXE = F$

$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}, C = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 1 & 7 & 10 & 2 & 6 & 9 & 8 \end{pmatrix}.$

$D = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix}, E = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 7 & 4 & 5 & 6 \end{pmatrix},$

$F = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 3 & 6 & 4 & 7 & 2 \end{pmatrix}.$

[ a) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$; b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$; c) $C^{100} = C$; d) $X = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$ ]

**5.3** Zjistěte, je-li následující součin členem determinantu příslušného stupně. Pokud je členem, určete jeho znaménko.

a) $a_{13}a_{22}a_{34}a_{24}a_{41}a_{56}$; b) $a_{32}a_{51}a_{13}a_{45}a_{24}$

[ a) není; b) je +1 ]

**5.4** Vypočítejte determinant

a) $\begin{vmatrix} 3 & -5 \\ 4 & 2 \end{vmatrix}$; b) $\begin{vmatrix} 2 & -1 & 8 \\ 4 & 1 & -2 \\ 1 & 4 & 3 \end{vmatrix}$; c) $\begin{vmatrix} a & b & c \\ c & a & b \\ b & c & a \end{vmatrix}$.

[ a) 26; b) 156; c) $a^3 + b^3 + c^3 - 3abc$ ]

**5.5** Vypočítejte determinant

a) $\begin{vmatrix} 5 & 9 & 2 & 7 \\ 4 & -5 & -3 & 2 \\ -3 & 5 & 1 & -4 \\ 5 & 4 & 3 & 5 \end{vmatrix}$; b) $\begin{vmatrix} 2 & -5 & 4 & 3 \\ 3 & -4 & 7 & 5 \\ 4 & -9 & 8 & 5 \\ -3 & 2 & -5 & 3 \end{vmatrix}$

[ a) -560; b) 4 ]

**5.6** Vypočítejte determinant $n$-tého stupně

$$\text{a)} \begin{vmatrix} 2 & 5 & 0 & 0 & \cdots & 0 & 0 \\ 2 & 7 & 5 & 0 & \cdots & 0 & 0 \\ 0 & 2 & 7 & 5 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 7 & 5 \\ 0 & 0 & 0 & 0 & \cdots & 2 & 7 \end{vmatrix}; \qquad \text{b)} \begin{vmatrix} 0 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & x & \cdots & x & x \\ 1 & x & 0 & \cdots & x & x \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & x & x & \cdots & 0 & x \\ 1 & x & x & \cdots & x & 0 \end{vmatrix}$$

[ a) $2^n$; b) $(-1)^{n-1} \cdot (n-1) \cdot x^{n-2}$ ]

**5.7** Vypočítejte následující determinanty

$$A = \begin{vmatrix} \frac{3}{2} & -\frac{3}{2} & -\frac{5}{2} & 4 \\ -1 & \frac{2}{3} & \frac{4}{3} & -2 \\ \frac{2}{3} & -\frac{5}{3} & -\frac{7}{3} & \frac{10}{6} \\ -4 & 3 & 5 & -6 \end{vmatrix}; \qquad B = \begin{vmatrix} \frac{3}{2} & -\frac{9}{2} & -\frac{3}{2} & -3 \\ \frac{5}{3} & -\frac{8}{3} & -\frac{2}{3} & -\frac{7}{3} \\ \frac{4}{3} & -\frac{5}{3} & -1 & -\frac{2}{3} \\ 7 & -8 & -4 & -5 \end{vmatrix}; \qquad C = \begin{vmatrix} 1 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 3 & 2 \\ 2 & 2 & 2 & 4 \end{vmatrix};$$

$$D = \begin{vmatrix} 2 & 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 \end{vmatrix}; \qquad E = \begin{vmatrix} 3 & 2 & 2 & 2 \\ 2 & 3 & 2 & 2 \\ 2 & 2 & 3 & 2 \\ 2 & 2 & 2 & 3 \end{vmatrix}; \qquad F = \begin{vmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ 1 & 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 0 \end{vmatrix};$$

$$G = \begin{vmatrix} 1 & n & n & \cdots & n \\ n & 2 & n & \cdots & n \\ n & n & 3 & \cdots & n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ n & n & n & \cdots & n \end{vmatrix}; \; H = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ 1 & 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 0 \end{vmatrix}; \; I = \begin{vmatrix} 1 & a_1 & a_2 & \cdots & a_n \\ 1 & b_1 + a_1 & a_2 & \cdots & a_n \\ 1 & a_1 & b_2 + a_2 & \cdots & a_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_1 & a_2 & \cdots & b_n + a_n \end{vmatrix};$$

$$J = \begin{vmatrix} 1 & 1 & \cdots & 1 & -n \\ 1 & 1 & \cdots & -n & 1 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 1 & -n & \cdots & 1 & 1 \\ -n & 1 & \cdots & 1 & 1 \end{vmatrix}.$$

[ $\det A = 1$; $\det B = 1$; $\det C = -4$; $\det D = 6$; $\det E = 9$; $\det F = (-1)^{n-1}(n-1)$; $\det G = (-1)^{n-1} n!$; $\det H = (-1)^{n-1}$; $\det I = b_1 b_2 \dots b_n$; $\det J = (-1)^{\frac{n(n+1)}{2}} (n+1)^{n-1}$ ]

**5.8** Nechť

$$A = \begin{pmatrix} a^2 + 1 & ab & ac \\ ab & b^2 + 1 & bc \\ ac & bc & c^2 + 1 \end{pmatrix}.$$

Vypočítejte determinant matice $A^2$.
[ $(a^2 + b^2 + c^2 + 1)^2$ ]

# Kapitola 6

# Vektorové prostory

Ve 4. kapitole jsme se již zabývali aritmetickými vektorovými prostory. Jejich prvky byly uspořádané $n$-tice ($n \in \mathbb{N}$) čísel z některého číselného tělesa $\mathcal{T}$ uvažovaného spolu se sčítáním těchto $n$-tic a s násobením $n$-tic prvky z tělesa (tj. násobení skaláry). Nyní si ukážeme, že aritmetické vektorové prostory jsou jen speciálním případem obecnějších vektorových prostorů, které se v matematice vyskytují velmi často.

## 6.1 Vektorové prostory a podprostory

**Definice 6.1** *Jsou-li $A$ a $B$ neprázdné množiny, potom* levou vnější operací *nad množinami $A$ a $B$ (v tomto pořadí) rozumíme každé zobrazení $\circ : A \times B \to B$. (Jsou-li $a \in A$, $b \in B$, pak prvek $\circ(a, b)$ budeme označovat $a \circ b$).*

`Poznámka:` Vidíme, že na rozdíl od (binární) operace na dané množině, která každé uspořádané dvojici prvků z této množiny přiřazuje jednoznačně prvek z téže množiny, levá vnější operace každé uspořádané dvojici prvků ze dvou různých množin přiřazuje prvek z druhé z uvažovaných množin.

Příkladem levé vnější operace může být součin skaláru a matice, kde ve výsledku dostáváme vždy matici.

**Definice 6.2** *Nechť $(V, +)$ je komutativní grupa (její prvky budeme označovat např. $\overrightarrow{u}$, $\overrightarrow{v}$, nulový prvek $\overrightarrow{o}$), $\mathcal{T}$ číselné těleso, $\circ : T \times V \longrightarrow V$ levá vnější operace nad $T$ a $V$. Potom systém $\mathcal{V} = (V, +, \mathcal{T}, \circ)$ nazveme* vektorový prostor nad tělesem $\mathcal{T}$, *platí-li*

1. $\forall c \in T, \overrightarrow{u}, \overrightarrow{v} \in V; c \circ (\overrightarrow{u} + \overrightarrow{v}) = c \circ \overrightarrow{u} + c \circ \overrightarrow{v}$,
2. $\forall c, d \in T, \overrightarrow{u} \in V; (c + d) \circ \overrightarrow{u} = c \circ \overrightarrow{u} + d \circ \overrightarrow{v}$,
3. $\forall c, d \in T, \overrightarrow{u} \in V; (cd) \circ \overrightarrow{u} = c \circ (d \circ \overrightarrow{v})$,
4. $\forall \overrightarrow{u} \in V; 1 \circ \overrightarrow{u} = \overrightarrow{u}$.

*Prvky z komutativní grupy* $(V, +)$ *budeme nazývat* vektory, *čísla z tělesa* $\mathcal{T}$ skaláry, *množinu* $V$ *nazveme* pole *vektorového prostoru* $\mathcal{V}$.

`Poznámka`: Protože není nebezpečí nedorozumění, označujeme v definici stejným symbolem „+“ operací sčítání v grupě $(V, +)$ i sčítání čísel v tělese $\mathcal{T}$. Pro jednoduchost budeme také levou vnější operaci „$\circ$“ označovat stejně jako násobení čísel v $\mathcal{T}$ a budeme ji také nazývat *násobení vektoru skalárem*.

**Příklad 6.1**

a) Ve větě 4.3 je vlastně dokázáno, že množina $M_{n\times m}(\mathcal{T})$ uvažovaná spolu se sčítáním matic skaláry z $\mathcal{T}$, je vektorovým prostorem nad $\mathcal{T}$. Proto také každý aritmetický vektorový prostor nad $\mathcal{T}$ je vektorovým prostorem nad $\mathcal{T}$.

b) Označme $\mathcal{V}_3(\mathcal{R})$ množinu všech vektorů třírozměrného geometrického vektorového prostoru spolu s operací sčítání vektorů a s násobením vektorů reálnými čísly. Je zřejmé, že $\mathcal{V}_3(\mathcal{R})$ je vektorovým prostorem nad tělesem $\mathcal{R}$.

Nyní budeme obecně definovat některé pojmy, se kterými jsme se již setkali (a s kterými jsme již pracovali) ve speciálním případě aritmetických vektorových prostorů.

**Definice 6.3** *Je-li* $\mathcal{V}$ *vektorový prostor nad číselným tělesem* $\mathcal{T}$ *a jsou-li* $\overrightarrow{v}, \overrightarrow{u_1}, \ldots, \overrightarrow{u_k} \in V$, *pak řekneme, že vektor* $\overrightarrow{v}$ *je* lineární kombinací vektorů $\overrightarrow{u_1}, \ldots, \overrightarrow{u_k}$, *existují-li čísla* $c_1, \ldots, c_k \in T$ *taková, že platí*

$$\overrightarrow{v} = \sum_{i=1}^{k} c_i \overrightarrow{u_i}.$$

`Poznámka`: Obdobně jako pro aritmetické vektory, také pro vektory $\overrightarrow{u_1}, \ldots, \overrightarrow{u_k}$ z libovolného vektorového prostoru $\mathcal{V}$ nad $\mathcal{T}$ platí, že existuje alespoň jedna jejich nulová lineární kombinace (tj. taková jejich lineární kombinace, která je rovna nulovém vektoru $\overrightarrow{o}$). Vždy totiž můžeme uvažovat jejich triviální nulovou kombinaci

$$\overrightarrow{o} = 0 \cdot \overrightarrow{u_1} + \ldots + 0 \cdot \overrightarrow{u_k}.$$

Každou jejich jinou nulovou lineární kombinaci budeme opět nazývat netriviální nulová kombinace.

**Definice 6.4** *Vektory* $\overrightarrow{u_1}, \ldots, \overrightarrow{u_k}$ *z vektorového prostoru* $\mathcal{V}$ *se nazývají* lineárně závislé, *existuje-li alespoň jedna jejich netriviální nulová kombinace.*

*V opačném případě se vektory* $\overrightarrow{u_1}, \ldots, \overrightarrow{u_k}$ *nazývají* lineárně nezávislé.

`Poznámka`: Je-li $\overrightarrow{u}$ vektor z $\mathcal{V}$ , pak $\overrightarrow{u}$ je lineárně nezávislý právě tehdy, když $\overrightarrow{u} \neq \overrightarrow{o}$.

**Věta 6.1** *Jsou-li mezi vektory* $\overrightarrow{u_1}, \ldots, \overrightarrow{u_m}$ *z vektorového prostoru některé vektory lineárně závislé, pak jsou také vektory* $\overrightarrow{u_1}, \ldots, \overrightarrow{u_m}$ *lineárně závislé.*

D ů k a z: Předpokládejme bez újmy na obecnosti, že vektory $\overrightarrow{u_1}, \dots, \overrightarrow{u_k}$ $(k < m)$ jsou lineárně závislé. Potom musí existovat $c_1, \dots, c_k \in T$ taková, že

$$\sum_{i=1}^{k} c_i \overrightarrow{u_i} = \overrightarrow{o},$$

a přitom alespoň jedno z čísel $c_1, \dots, c_k$ je různé od nuly. Pak ale také platí

$$\sum_{i=1}^{k} c_i \overrightarrow{u_i} + \sum_{j=k+1}^{m} 0 \cdot \overrightarrow{u_j} = \overrightarrow{o},$$

tedy existuje také netriviální nulová lineární kombinace vektorů $\overrightarrow{u_1}, \dots, \overrightarrow{u_k}, \dots, \overrightarrow{u_m}$, tzn., že tyto vektory jsou také lineárně závislé. □

Na základě zákona kontrapozice z výrokové logiky platí proto také věta obměněná k větě 6.1:

**Věta 6.2** *Jsou-li vektory $\overrightarrow{u_1}, \dots, \overrightarrow{u_m}$ lineárně nezávislé a je-li $\{\overrightarrow{u_{j_1}}, \dots, \overrightarrow{u_{j_k}}\}$ podmnožinou množiny $\{\overrightarrow{u_1}, \dots, \overrightarrow{u_m}\}$, potom jsou lineárně nezávislé také vektory $\overrightarrow{u_{j_1}}, \dots, \overrightarrow{u_{j_k}}$.* □

**Věta 6.3** *Jsou-li $\overrightarrow{u_1}, \dots, \overrightarrow{u_k}$ vektory z vektorového prostoru $\mathcal{V}$, pak jsou tyto vektory lineárně závislé právě tehdy, je-li alespoň jeden z těchto vektorů lineární kombinací ostatních vektorů.*

D ů k a z:

a) Nechť $\overrightarrow{u_1}, \dots, \overrightarrow{u_k}$ jsou lineárně závislé. Pak existují čísla $c_1, \dots, c_k \in T$ taková, že

$$\sum_{i=1}^{k} c_i \overrightarrow{u_i} = \overrightarrow{o},$$

a přitom můžeme najít $j \in \{1, \dots, k\}$, pro které platí $c_j \neq 0$. Pak ale platí

$$\overrightarrow{u_j} = \sum_{i=1, i \neq j}^{k} (-\frac{c_i}{c_j}) \overrightarrow{u_i},$$

a tedy $\overrightarrow{u_j}$ je lineární kombinací zbývajících vektorů.

b) Jestliže vektor $\overrightarrow{u_j}$ je lineární kombinací vektorů $\overrightarrow{u_1}, \dots, \overrightarrow{u_{j-1}}, \overrightarrow{u_{j+1}}, \dots, \overrightarrow{u_k}$, pak existují čísla $c_1, \dots, c_{j-1}, c_{j+1}, \dots, c_k \in T$ taková, že

$$\overrightarrow{u_j} = \sum_{i=1, i \neq j}^{k} c_i \overrightarrow{u_i},$$

tj. platí

$$\sum_{i=1}^{j-1} c_i \overrightarrow{u_i} + (-1)\overrightarrow{u_j} + \sum_{p=j+1}^{k} c_p \overrightarrow{u_p} = \overrightarrow{o},$$

a tato nulová lineární kombinace vektorů $\overrightarrow{u_1}, \dots, \overrightarrow{u_k}$ je netriviální, proto jsou vektory $\overrightarrow{u_1}, \dots, \overrightarrow{u_k}$ lineárně závislé.

□

Uvažujme podmnožinu $A = \{(x, y, 0); x, y \in \mathbb{R}\}$ kartézské mocniny $\mathbb{R}^3$. Je zřejmé, že vzhledem ke sčítání uspořádaných trojic z $A$ a vzhledem k násobení těchto trojic reálnými čísly tvoří $A$ vektorový prostor nad $\mathcal{R}$. Přitom každý z vektorů tohoto prostoru je také vektorem z aritmetického vektorového prostoru $\mathcal{R}^3$. Nyní se obecně budeme věnovat analogickým vztahům mezi vektorovými prostory.

**Definice 6.5** *Řekneme, že vektorový prostor $\mathcal{W} = (W, \oplus, \mathcal{T}, \circ)$ je* podprostorem *vektorového prostoru $\mathcal{V} = (V, +, \mathcal{T}, \cdot)$, platí-li*

*a)* $W \subseteq V$,

*b)* $\forall \overrightarrow{u}, \overrightarrow{v} \in W; \overrightarrow{u} \oplus \overrightarrow{v} = \overrightarrow{u} + \overrightarrow{v}$,

*c)* $\forall c \in T, \overrightarrow{u} \in W; c \circ \overrightarrow{u} = c\overrightarrow{u}$.

*(Je-li $\mathcal{W}$ podprostorem prostoru $\mathcal{V}$, pak píšeme $\mathcal{W} \subseteq\subseteq \mathcal{V}$.)*

`Poznámka`: Znamená to, že prostor $\mathcal{W}$ je podprostorem prostoru $\mathcal{V}$, je-li $W$ neprázdnou podmnožinou množiny $\mathcal{V}$ a vzniknou-li operace sčítání vektorů a vnější operace násobení vektorů skaláry z $T$ v prostoru $\mathcal{W}$ z odpovídajících operací ve $\mathcal{V}$ omezením se na množinu $W$.

**Příklad 6.2**

a) Vektorový prostor geometrických vektorů v rovině je podprostorem vektorového prostoru geometrických vektorů v třírozměrném prostoru.

b) Označme $D_n(\mathcal{T})$ množinu všech diagonálních matic stupně $n$ nad $\mathcal{T}$. Je zřejmé, že $D_n(\mathcal{T})$ spolu se sčítáním matic a s násobením matic skaláry z $T$ je vektorovým prostorem nad $\mathcal{T}$. (Označíme jej $\mathcal{D}_n(\mathcal{T})$.) Přitom platí, že $\mathcal{D}_n(\mathcal{T}) \subseteq\subseteq \mathcal{M}_n(\mathcal{T})$.

c) Je zřejmé, že pro každý vektorový prostor $\mathcal{V}$ je $\{\overrightarrow{o}\}$ podprostorem ve $\mathcal{V}$. Vzhledem k tomu, že nulový vektor $\overrightarrow{o}$ musí patřit do každého podprostoru $\mathcal{W}$ prostoru $\mathcal{V}$, platí vždy $\{\overrightarrow{o}\} \subseteq\subseteq \mathcal{V}$.

**Věta 6.4** *Podmnožina $W \neq \emptyset$ vektorového prostoru $\mathcal{V}$ je polem podprostoru $\mathcal{W} \subseteq\subseteq \mathcal{V}$ právě tehdy, platí-li*

1. $\forall \overrightarrow{u}, \overrightarrow{v} \in W; \overrightarrow{u} + \overrightarrow{v} \in W$,

2. $\forall c \in T, \overrightarrow{u} \in W; c\overrightarrow{u} \in W$.

D ů k a z: Jestliže platí podmínky 1 a 2, pak „+“ omezená na $W$ je operací na $W$. Tato operace je asociativní a komutativní, protože tyto vlastnosti má sčítání na $V$. Je-li $\overrightarrow{u} \in W$, pak podle 2 platí $-\overrightarrow{u} = (-1)\overrightarrow{u} \in W$, a podle 1 také $\overrightarrow{o} = \overrightarrow{u} + (-\overrightarrow{u}) \in W$. To znamená, že $(W, +)$ je komutativní grupa. Dále podle 2 platí, že násobení vektorů z $W$ skaláry z $T$ je levou vnější operací nad $T$ a $V$, a proto podmínky 1-4 z definice 6.2 jsou opět splněny triviálně. Tedy $\mathcal{W}$ je vektorovým prostorem nad $\mathcal{T}$ a protože $W \subseteq V$, platí $\mathcal{W} \subseteq\subseteq \mathcal{V}$.

Obrácená implikace je zřejmá. □

**Věta 6.5** *Průnik libovolného systému $\{\mathcal{W}_\alpha; \alpha \in I\}$ podprostorů vektorového prostoru $\mathcal{V}$ je podprostorem $\mathcal{V}$.*

D ů k a z: Označme $W = \bigcap\limits_{\alpha \in I} W_\alpha$. Protože pro každé $\alpha \in I$ platí $\overrightarrow{o} \in W_\alpha$, je $W \neq \emptyset$. Nechť $\overrightarrow{u}, \overrightarrow{v} \in W$. Pak $\overrightarrow{u}, \overrightarrow{v} \in W_\alpha$ pro každé $\alpha \in I$, a proto také $\overrightarrow{u} + \overrightarrow{v} \in W_\alpha$ pro každé $\alpha \in I$, tedy $\overrightarrow{u} + \overrightarrow{v} \in W$. Analogicky, jestliže $c \in T$, $\overrightarrow{u} \in W$, pak $\overrightarrow{u} \in W_\alpha$ pro každé $\alpha \in I$, a tedy $c\overrightarrow{u} \in W_\alpha$ pro každé $\alpha \in I$, což znamená, že $c\overrightarrow{u} \in W$. Podle věty 6.4 je tedy $W$ polem podprostoru $\mathcal{W}$ vektorového prostoru $\mathcal{V}$. □

`Poznámka`: Podprostor $\mathcal{W} = \bigcap\limits_{\alpha \in I} \mathcal{W}_\alpha$ je tedy největším podprostorem v prostoru $\mathcal{V}$, který je obsažen ve všech podprostorech $\mathcal{W}_\alpha, \alpha \in I$.

**Definice 6.6** *Je-li $M$ podmnožina vektorového prostoru $\mathcal{V}$, pak* lineárním obalem množiny $M$ ve $\mathcal{V}$ *rozumíme průnik všech podprostorů prostoru $\mathcal{V}$ obsahujících množinu $M$. (Lineární obal množiny $M$ označíme $[M]$.)*

`Poznámka`: Podle věty 6.5 platí, že $[M]$ je podprostorem prostoru $\mathcal{V}$. Přitom je zřejmé, že je to nejmenší podprostor prostoru $\mathcal{V}$, který obsahuje $M$. (Tzn., jestliže $M \subseteq \mathcal{W}$, pak $[M] \subseteq\subseteq \mathcal{W}$.)

**Věta 6.6** *Nechť $M$ je podmnožina vektorového prostoru $\mathcal{V}$ nad $\mathcal{T}$. Pak platí*

*a) Jestliže $M \neq \emptyset$, pak $[M] = \{\overrightarrow{o}\}$.*

*b) Jestliže $M \neq \emptyset$, pak $[M] = \{\overrightarrow{v} \in V; \overrightarrow{v} = \sum\limits_{i=1}^{k} c_i \overrightarrow{u_i}, k \in N, c_i \in T, \overrightarrow{u_i} \in M, i = 1, \ldots, k\}$.*

D ů k a z: Případ a) je zřejmý.

b) Nechť $\emptyset \neq M \subseteq V$. Označme

$$W = \{\overrightarrow{u} \in V; \overrightarrow{u} = \sum_{i=1}^{k} c_i \overrightarrow{u_i}, k \in N, c_i \in T, \overrightarrow{u_i} \in M, i = 1, \ldots, k\}.$$

Jsou-li $\overrightarrow{u}, \overrightarrow{v} \in W$, pak existují $k, m \in N$, $c_i, d_j \in T$, $\overrightarrow{u_i}, \overrightarrow{v_j} \in M$, $i = 1, \ldots, k$, $j = 1, \ldots, m$ tak, že

$$\overrightarrow{u} = \sum_{i=1}^{k} c_i \overrightarrow{u_i}, \qquad \overrightarrow{v} = \sum_{j=1}^{m} d_j \overrightarrow{v_j}.$$

Tedy

$$\overrightarrow{u} + \overrightarrow{v} = \sum_{i=1}^{k} c_i \overrightarrow{u_i} + \sum_{j=1}^{m} d_j \overrightarrow{v_j},$$

a proto $\overrightarrow{u} + \overrightarrow{v} \in W$.
Jestliže $c \in T$, $\overrightarrow{u} = \sum_{i=1}^{k} c_i \overrightarrow{u_i} \in W$, pak

$$c\overrightarrow{u} = c \cdot \sum_{i=1}^{k} c_i \overrightarrow{u_i} = \sum_{i=1}^{k} (cc_i) \overrightarrow{u_i},$$

a protože $cc_i \in T$, $\overrightarrow{u_i} \in M$ $(i = 1, \ldots, n)$, platí $c\overrightarrow{u} \in W$.
Tedy $W$ je polem podprostoru $\mathcal{W}$ prostoru $\mathcal{V}$. Přitom pro každý $\overrightarrow{u} \in M$ platí $\overrightarrow{u} = 1 \cdot \overrightarrow{u} \in W$, proto $M \subseteq W$. Jestliže je $\mathcal{W}'$ libovolný podprostor prostoru $\mathcal{V}$, který obsahuje množinu $M$, pak pro každý $\overrightarrow{u_i} \in M$ platí $\overrightarrow{u_i} \in W'$. Protože $\mathcal{W}'$ je prostor, platí $c_i \overrightarrow{u_i} \in W'$, a tedy také

$$\overrightarrow{u} = \sum_{i=1}^{k} c_i \overrightarrow{u_i} \in W' \qquad (c_i \in T, \overrightarrow{u_i} \in M, i = 1, \ldots, k).$$

To ovšem znamená, že $\mathcal{W} \subseteq\subseteq \mathcal{W}'$, proto platí $\mathcal{W} = [M]$.

□

`Poznámka`: Podle předchozí věty je pro neprázdnou podmnožinu $M$ prostoru $\mathcal{V}$ jejím lineárním obalem $[M]$ podprostor ve $\mathcal{V}$, který se skládá právě ze všech konečných lineárních kombinací vektorů z množiny $M$.

Nechť nyní $\mathcal{W}_1$ a $\mathcal{W}_2$ jsou dva podprostory vektorového prostoru $\mathcal{V}$. Ukažme, že v takovém případě můžeme určit nejmenší podprostor ve $\mathcal{V}$, který obsahuje oba podprostory $\mathcal{W}_1$ a $\mathcal{W}_2$ (tedy lineární obal množiny $\mathcal{W}_1 \cup \mathcal{W}_2$) jednodušeji, než umožňuje věta 6.6.

**Věta 6.7** *Jsou-li $\mathcal{W}_1$ a $\mathcal{W}_2$ podprostory vektorového prostoru $\mathcal{V}$ nad $\mathcal{T}$, potom polem nejmenšího podprostoru, který obsahuje $\mathcal{W}_1$ a $\mathcal{W}_2$ je množina $W_1 + W_2 = \{\overrightarrow{v} \in V; \overrightarrow{v} = \overrightarrow{v_1} + \overrightarrow{v_2}$, kde $\overrightarrow{v_1} \in W_1, \overrightarrow{v_2} \in W_2\}$.*

D ů k a z: Podle věty 6.6 je zřejmé, že $W_1 + W_2 \subseteq [W_1 \cup W_2]$. Přitom pro libovolný vektor $\overrightarrow{v_1} \in W_1$ platí $\overrightarrow{v_1} = \overrightarrow{v_1} + \overrightarrow{o}$, a protože $\overrightarrow{o} \in W_2$, musí platit, že $\overrightarrow{v_1} \in W_1 + W_2$. Proto $W_1 \subseteq W_1 + W_2$. Analogicky můžeme dokázat, že $W_2 \subseteq W_1 + W_2$.

K důkazu tvrzení tedy stačí ověřit, že $W_1 + W_2$ je polem podprostoru v prostoru $\mathcal{V}$. Nechť $\overrightarrow{u}, \overrightarrow{v} \in W_1 + W_2$. Pak existují $\overrightarrow{u_1}, \overrightarrow{v_1} \in W_1$, $\overrightarrow{u_2}, \overrightarrow{v_2} \in W_2$ takové, že $\overrightarrow{u} = \overrightarrow{u_1} + \overrightarrow{u_2}$, $\overrightarrow{v} = \overrightarrow{v_1} + \overrightarrow{v_2}$. Protože $(V, +)$ je komutativní grupa, platí

$$\overrightarrow{u} + \overrightarrow{v} = (\overrightarrow{u_1} + \overrightarrow{u_2}) + (\overrightarrow{v_1} + \overrightarrow{v_2}) = (\overrightarrow{u_1} + \overrightarrow{v_1}) + (\overrightarrow{u_2} + \overrightarrow{v_2}),$$

a podle věty 6.4 je $\overrightarrow{u_1} + \overrightarrow{v_1} \in W_1$, $\overrightarrow{u_2} + \overrightarrow{v_2} \in W_2$. Tedy $\overrightarrow{u} + \overrightarrow{v} \in W_1 + W_2$.

Předpokládejme nyní, že $c \in T$, $\overrightarrow{u} = \overrightarrow{u_1} + \overrightarrow{u_2} \in W_1 + W_2$. Pak

$$c\overrightarrow{u} = c(\overrightarrow{u_1} + \overrightarrow{u_2}) = c\overrightarrow{u_1} + c\overrightarrow{u_2},$$

a odtud opět podle věty 6.4 dostáváme, že $c\overrightarrow{u} \in W_1 + W_2$. □

**Definice 6.7** *Podprostor ve $\mathcal{V}$, jehož polem je množina $W_1 + W_2$, označíme $\mathcal{W}_1 + \mathcal{W}_2$ a nazveme jej* součet podprostorů *$\mathcal{W}_1$ a $\mathcal{W}_2$.*

**Definice 6.8** *Platí-li pro podprostory $\mathcal{W}_1$ a $\mathcal{W}_2$ vektorového prostoru $\mathcal{V}$, že $\mathcal{W}_1 + \mathcal{W}_2 = \mathcal{V}$ a $\mathcal{W}_1 \cap \mathcal{W}_2 = \{\overrightarrow{o}\}$, pak řekneme, že prostor $\mathcal{V}$ je* přímým součtem *svých prostorů $\mathcal{W}_1$ a $\mathcal{W}_2$. (Značíme $\mathcal{V} = \mathcal{W}_1 \dot{+} \mathcal{W}_2$.)*

**Věta 6.8** *Je-li vektorový prostor $\mathcal{V}$ přímým součtem podprostorů $\mathcal{W}_1$ a $\mathcal{W}_2$, pak každý vektor $\overrightarrow{v} \in V$ je možno vyjádřit právě jedním způsobem ve tvaru $\overrightarrow{v} = \overrightarrow{v_1} + \overrightarrow{v_2}$, kde $\overrightarrow{v_1} \in \mathcal{W}_1$, $\overrightarrow{v_2} \in \mathcal{W}_2$.*

D ů k a z: Jestliže $\mathcal{V} = \mathcal{W}_1 \dot{+} \mathcal{W}_2$, pak platí mj. $\mathcal{V} = \mathcal{W}_1 + \mathcal{W}_2$, a proto podle věty 6.7 každý vektor $\overrightarrow{v} \in V$ je možno vyjádřit alespoň jedním způsobem v požadovaném tvaru $\overrightarrow{v} = \overrightarrow{v_1} + \overrightarrow{v_2}$. Ukažme, že takové vyjádření je jednoznačné.

Nechť $\overrightarrow{v} = \overrightarrow{v_1} + \overrightarrow{v_2}$, $\overrightarrow{v} = \overrightarrow{u_1} + \overrightarrow{u_2}$, kde $\overrightarrow{u_1}, \overrightarrow{v_1} \in W_1$, $\overrightarrow{u_2}, \overrightarrow{v_2} \in W_2$. Pak

$$\overrightarrow{v_1} + \overrightarrow{v_2} = \overrightarrow{u_1} + \overrightarrow{u_2},$$

a tedy

$$\overrightarrow{v_1} - \overrightarrow{u_1} = \overrightarrow{u_2} - \overrightarrow{v_2}.$$

Ovšem platí $\overrightarrow{v_1} - \overrightarrow{u_1} \in W_1$, $\overrightarrow{u_2} - \overrightarrow{v_2} \in W_2$, a protože $\mathcal{V} = \mathcal{W}_1 \dot{+} \mathcal{W}_2$ (tedy $W_1 \cap W_2 = \{\overrightarrow{o}\}$), musí nastat $\overrightarrow{v_1} - \overrightarrow{u_1} = \overrightarrow{o}$, $\overrightarrow{u_2} - \overrightarrow{v_2} = \overrightarrow{o}$. Odtud $\overrightarrow{v_1} = \overrightarrow{u_1}$ a $\overrightarrow{v_2} = \overrightarrow{u_2}$. □

## 6.2 Vektorové prostory konečné dimenze

**Definice 6.9** *Nechť $\mathcal{V}$ je vektorový prostor nad číselným tělesem $\mathcal{T}$. Platí-li pro podmnožinu $M \neq \emptyset$ prostoru $\mathcal{V}$, že $[M] = \mathcal{V}$, pak $M$ se nazývá* množina generátorů prostoru *$\mathcal{V}$. (Říkáme také, že množina $M$* generuje prostor *$\mathcal{V}$).*

`Poznámka`: Každý vektor z $\mathcal{V}$ se dá tedy vyjádřit ve tvaru lineární kombinace vektorů z množiny generátorů.

**Definice 6.10** *Řekneme, že vektorový prostor $\mathcal{V}$ je* konečné dimenze, *jestliže existuje alespoň jedna jeho konečná množina generátorů.*

**Definice 6.11** Bází *vektorového prostoru $\mathcal{V}$ konečné dimenze rozumíme libovolnou lineárně nezávislou množinu $\{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ jeho generátorů.*

`Poznámka`:

a) Je zřejmé, že množina $\{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ je bází vektorového prostoru $\mathcal{V}$ právě tehdy, je-li maximální lineárně nezávislou podmnožinou ve $\mathcal{V}$.

b) Všude v dalším se budeme věnovat pouze vektorovým prostorům konečné dimenze.

**Věta 6.9** *Nechť $M = \{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ je báze vektorového prostoru $\mathcal{V}$. Pak každý vektor $\overrightarrow{v} \in \mathcal{V}$ je možno vyjádřit právě jedním způsobem ve tvaru lineární kombinace vektorů $\overrightarrow{u_1}, \dots, \overrightarrow{u_n}$.*

D ů k a z: Protože $M$ je množina generátorů vektorového prostoru $\mathcal{V}$, můžeme každý vektor $\overrightarrow{v} \in \mathcal{V}$ zapsat alespoň jedním způsobem ve tvaru lineární kombinace

$$\overrightarrow{v} = \sum_{i=1}^{n} c_i \overrightarrow{u_i}$$

vektorů $\overrightarrow{u_1}, \dots, \overrightarrow{u_n}$. Je-li

$$\overrightarrow{v} = \sum_{i=1}^{n} d_i \overrightarrow{u_i}$$

další takové vyjádření vektoru $\overrightarrow{v}$, pak platí

$$\overrightarrow{o} = \overrightarrow{v} - \overrightarrow{v} = \sum_{i=1}^{n} c_i \overrightarrow{u_i} - \sum_{i=1}^{n} d_i \overrightarrow{u_i} = \sum_{i=1}^{n} (c_i - d_i) \overrightarrow{u_i},$$

a protože vektory $\overrightarrow{u_1}, \dots, \overrightarrow{u_n}$ jsou lineárně nezávislé, musí nastat $c_i - d_i = 0$ pro každé $i = 1, \dots, n$, a to znamená, že $c_i = d_i$ pro každé $i = 1, \dots, n$. □

**Příklad 6.3** Nechť $\overrightarrow{e_1} = (1, 0, 0, 0)$, $\overrightarrow{e_2} = (0, 1, 0, 0)$, $\overrightarrow{e_3} = (0, 0, 1, 0)$, $\overrightarrow{e_4} = (0, 0, 0, 1)$. Platí, že množina $M = \{\overrightarrow{e_1}, \overrightarrow{e_2}, \overrightarrow{e_3}, \overrightarrow{e_4}\}$ je bází aritmetického vektorového prostoru $\mathcal{R}^4$, tedy každý z vektorů z $\mathcal{R}^4$ můžeme jednoznačně vyjádřit jako lineární kombinaci vektorů této báze.

Je-li $\overrightarrow{x} = \{x_1, x_2, x_3, x_4\} \in \mathcal{R}^4$, pak platí

$$\overrightarrow{x} = x_1 \overrightarrow{e_1} + x_2 \overrightarrow{e_2} + x_3 \overrightarrow{e_3} + x_4 \overrightarrow{x_4}.$$

Přitom ovšem $M$ není jedinou bází prostoru $\mathcal{R}^4$; brzy uvidíme, že bází v $\mathcal{R}^4$ je nekonečně mnoho.

**Věta 6.10** *Je-li $M = \{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ množina generátorů vektorového prostoru $\mathcal{V}$, pak existuje podmnožina $M' \subseteq M$, která je bází prostoru $\mathcal{V}$.*

D ů k a z: Předpokládejme, že $M = \{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ je množina generátorů prostoru $\mathcal{V}$, tj., že platí $[M] = \mathcal{V}$. Není-li $M$ bází prostoru $\mathcal{V}$, pak jsou vektory $\overrightarrow{u_1}, \dots, \overrightarrow{u_n}$ lineárně závislé, a tedy podle věty 6.3 existuje alespoň jeden vektor $\overrightarrow{u_i}$ ($i \in \{1, \dots, n\}$), který je lineární kombinací zbývajících vektorů. Pak ale můžeme vektor $\overrightarrow{u_i}$ vynechat, protože pro množinu $M_1 = M \setminus \{\overrightarrow{u_i}\}$ také platí, že $[M_1] = \mathcal{V}$. Je-li množina $M_1$ lineárně závislá, můžeme s ní provést analogický proces, který opakujeme do té doby, dokud nedostaneme lineárně nezávislou podmnožinu $M'$, která je pak bází prostoru $\mathcal{V}$. □

**Věta 6.11 Steinitzova věta** *Nechť $\{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ je množina generátorů vektorového prostoru $\mathcal{V} \neq \{\overrightarrow{o}\}$ a nechť $\overrightarrow{v_1}, \dots, \overrightarrow{v_k}$ jsou lineárně nezávislé vektory z $\mathcal{V}$. Potom platí, že $k \leq n$ a že po vhodném očíslování vektorů $\overrightarrow{u_1}, \dots, \overrightarrow{u_n}$ je množina $\{\overrightarrow{v_1}, \dots, \overrightarrow{v_k}, \overrightarrow{u_{k+1}}, \dots, \overrightarrow{u_n}\}$ množinou generátorů prostoru $\mathcal{V}$.*

D ů k a z: Budeme dokazovat indukcí podle počtu $k$ vektorů $\overrightarrow{v_1}, \dots, \overrightarrow{v_k}$.

a) Nechť $k = 1$. Protože vektor $\overrightarrow{v_1}$ je lineárně nezávislý, platí $v_1 \neq \overrightarrow{o}$. Podle předpokladu platí $[\{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}] = \mathcal{V}$ a protože $\overrightarrow{v_1} \in V$, existují $c_1, \dots, c_n \in T$ tak, že

$$\overrightarrow{v_1} = \sum_{i=1}^{n} c_i \overrightarrow{u_i}.$$

Přitom alespoň jedno z čísel $c_1, \dots, c_n$ je různé od nuly, neboť jinak by platilo $\overrightarrow{v_1} = \overrightarrow{o}$. Lze předpokládat, že $c_1 \neq 0$. (Jinak bychom vektory $\overrightarrow{u_1}, \dots, \overrightarrow{u_n}$ vhodně přečíslovali.) Pak platí

$$\overrightarrow{u_1} = \frac{1}{c_1}\overrightarrow{v_1} + \sum_{i=2}^{n}(-\frac{c_i}{c_1})\overrightarrow{u_i},$$

tedy $[\{\overrightarrow{v_1}, \overrightarrow{u_2}, \dots, \overrightarrow{u_n}\}] = \mathcal{V}$. Přitom zřejmě platí $1 \leq n$.

b) Nechť $k > 1$. Předpokládejme, že tvrzení platí pro všechna čísla $1, \dots, k-1$. Protože vektory $\overrightarrow{v_1}, \dots, \overrightarrow{v_k}$ jsou podle předpokladu lineárně nezávislé, jsou podle věty 6.2 lineárně nezávislé také vektory $\overrightarrow{v_1}, \dots, \overrightarrow{v_{k-1}}$. Proto podle indukčního předpokladu platí $k-1 \leq n$, a po vhodném očíslování vektorů $\overrightarrow{u_1}, \dots, \overrightarrow{u_n}$ je $\{\overrightarrow{v_1}, \dots, \overrightarrow{v_{k-1}}, \overrightarrow{u_k}, \dots, \overrightarrow{u_n}\}$ množinou generátorů prostoru $\mathcal{V}$. Musí tedy existovat $c_1, \dots, c_{k-1}, d_k, \dots, d_n \in T$ taková, že

$$\overrightarrow{v_k} = \sum_{i=1}^{k-1} c_i \overrightarrow{v_i} + \sum_{j=k}^{n} d_j \overrightarrow{u_j}.$$

Přitom alespoň jedno z čísel $d_k, \dots, d_n$ je nenulové, protože jinak by platilo

$$\overrightarrow{v_k} = \sum_{i=1}^{k-1} c_i \overrightarrow{v_i},$$

a tedy vektory $\overrightarrow{v_1}, \ldots, \overrightarrow{v_k}$ by nebyly lineárně nezávislé. Vektory $\overrightarrow{u_k}, \ldots, \overrightarrow{u_n}$ nyní vhodně očíslujeme tak, aby platilo $d_k \neq 0$. Potom z rovnosti

$$\overrightarrow{v_k} = \sum_{i=1}^{k-1} c_i \overrightarrow{v_i} + \sum_{j=k}^{n} d_j \overrightarrow{u_j}$$

vyplývá $k \leq n$ a přitom platí

$$\overrightarrow{u_k} = \sum_{i=1}^{k-1} (-\frac{c_i}{d_k}) \overrightarrow{v_i} + \frac{1}{d_k} \overrightarrow{v_k} + \sum_{j=k+1}^{n} (-\frac{d_j}{d_k}) \overrightarrow{u_j},$$

tedy $[\{\overrightarrow{v_1}, \ldots, \overrightarrow{v_k}, \overrightarrow{u_{k+1}}, \ldots, \overrightarrow{u_n}\}] = \mathcal{V}$.

□

**Věta 6.12** *Je-li $\mathcal{V} \neq \{\overrightarrow{o}\}$ vektorový prostor konečné dimenze, potom každé dvě jeho báze mají stejný počet prvků.*

D ů k a z: Nechť $\{\overrightarrow{u_1}, \ldots, \overrightarrow{u_n}\}$ a $\{\overrightarrow{v_1}, \ldots, \overrightarrow{v_k}\}$ jsou dvě báze vektorového prostoru $\mathcal{V}$. Potom podle Steinitzovy věty platí současně $k \leq n$ a $n \leq k$, tedy $n = k$. □

**Věta 6.13** *Nechť $[\{\overrightarrow{u_1}, \ldots, \overrightarrow{u_n}\}] = \mathcal{V}$ a nechť $\overrightarrow{v_1}, \ldots, \overrightarrow{v_k} \in V$. Je-li $k > n$, pak jsou vektory $\overrightarrow{v_1}, \ldots, \overrightarrow{v_k}$ lineárně závislé.*

D ů k a z: Tvrzení je bezprostředním důsledkem Steinitzovy věty, protože pokud by vektory $\overrightarrow{v_1}, \ldots, \overrightarrow{v_k}$ byly lineárně nezávislé, pak by muselo platit $k \leq n$. □

**Definice 6.12**

*a) Je-li $\mathcal{V} \neq \{\overrightarrow{o}\}$ vektorový prostor konečné dimenze, pak počet prvků jeho libovolné báze nazýváme* dimenze prostoru $\mathcal{V}$ *a značíme* $\dim \mathcal{V}$.

*b) Je-li $\mathcal{V} = \{\overrightarrow{o}\}$, pak* $\dim \mathcal{V} = 0$.

**Příklad 6.4** Podle příkladu 6.3 víme, že množina $M = \{\overrightarrow{e_1}, \overrightarrow{e_2}, \overrightarrow{e_3}, \overrightarrow{e_4}\}$ je bází aritmetického vektorového prostoru $\mathcal{R}^4$, tedy platí $\dim \mathcal{R}^4 = 4$.

Analogicky pro libovolné $n \geq 1$ platí, že $\dim \mathcal{R}^n = n$, protože jednu z bází tohoto prostoru tvoří množina složená z vektorů

$$\overrightarrow{e_1} = (1, 0, \ldots, 0), \overrightarrow{e_2} = (0, 1, \ldots, 0), \ldots, \overrightarrow{e_n} = (0, 0, \ldots, 1).$$

**Věta 6.14** *Nechť $[\{\overrightarrow{u_1}, \ldots, \overrightarrow{u_n}\}] = \mathcal{V}$. Potom platí* $\dim \mathcal{V} \leq n$.

D ů k a z: Tvrzení bezprostředně vyplývá z definice dimenze a ze Steinitzovy věty. □

**Věta 6.15** *Nechť* $\dim \mathcal{V} = n$ *a nechť* $\overrightarrow{u_1}, \dots, \overrightarrow{u_n} \in \mathcal{V}$. *Pak jsou následující podmínky ekvivalentní:*

*a)* $\overrightarrow{u_1}, \dots, \overrightarrow{u_n}$ *jsou lineárně nezávislé;*

*b)* $[\{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}] = \mathcal{V}$*;*

*c)* $\{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ *je báze prostoru* $\mathcal{V}$*.*

D ů k a z:

$a \Rightarrow b$: Je-li $\{\overrightarrow{v_1}, \dots, \overrightarrow{v_n}\}$ libovolná báze prostoru $\mathcal{V}$, potom podle Steinitzovy věty platí

$$[\{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}] = [\{\overrightarrow{v_1}, \dots, \overrightarrow{v_n}\}] = \mathcal{V}.$$

$b \Rightarrow c$: Jestliže $[\{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}] = \mathcal{V}$, pak vektory $\overrightarrow{u_1}, \dots, \overrightarrow{u_n}$ musí být lineárně nezávislé, protože jinak by podle věty 6.14 platilo $n = \dim \mathcal{V} < n$, spor.

$c \Rightarrow a$: Tato implikace plyne přímo z definice báze.

□

**Věta 6.16** *Je-li* $\mathcal{V}$ *vektorový prostor konečné dimenze* $n$*, pak každá množina* $\overrightarrow{u_1}, \dots, \overrightarrow{u_k}$ *lineárně nezávislých vektorů prostoru* $\mathcal{V}$ *je obsažena v některé bázi prostoru* $\mathcal{V}$*.*

D ů k a z: Víme, že $k \leq n$. Jestliže $k = n$, pak množina $\{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ je podle předchozí věty bází ve $\mathcal{V}$.

Nechť $k < n$. Uvažujme libovolnou bázi $\{\overrightarrow{v_1}, \dots, \overrightarrow{v_n}\}$ prostoru $\mathcal{V}$. Pak podle Steinitzovy věty po vhodném očíslování platí, že $[\{\overrightarrow{u_1}, \dots, \overrightarrow{u_k}, \overrightarrow{v_{k+1}}, \dots, \overrightarrow{v_n}\}] = \mathcal{V}$, a podle věty 6.15 je proto množina $\{\overrightarrow{u_1}, \dots, \overrightarrow{u_k}, \overrightarrow{v_{k+1}}, \dots, \overrightarrow{v_n}\}$ bází prostoru $\mathcal{V}$. □

**Věta 6.17** *Je-li* $\mathcal{W}$ *podprostor vektorového prostoru* $\mathcal{V}$ *konečné dimenze, pak* $\dim \mathcal{W} \leq \mathcal{V}$*. Přitom platí* $\dim \mathcal{W} = \dim \mathcal{V}$ *právě tehdy, když* $\mathcal{W} = \mathcal{V}$*.*

D ů k a z: Je zřejmé, že pokud jsou některé vektory z $W$ lineárně nezávislé ve $\mathcal{W}$, pak jsou lineárně nezávislé také v celém prostoru $\mathcal{V}$. Je-li tedy $\dim \mathcal{V} = n$, pak každá lineárně nezávislá množina vektorů podprostoru $\mathcal{W}$ má podle věty 6.13 nejvýše $n$ prvků, což znamená, že $\dim \mathcal{W} \leq \dim \mathcal{V}$.

Druhá část tvrzení je přímým důsledkem věty 6.15. □

**Věta 6.18** *Nechť $\mathcal{W}_1$ a $\mathcal{W}_2$ jsou podprostory konečné dimenze vektorového prostoru $\mathcal{V}$. Potom platí*

$$\dim \mathcal{W}_1 + \dim \mathcal{W}_2 = \dim(\mathcal{W}_1 + \mathcal{W}_2) + \dim(\mathcal{W}_1 \cap \mathcal{W}_2).$$

D ů k a z: Nechť $\dim \mathcal{W}_1 = k$,$\dim \mathcal{W}_2 = l$, $\dim(\mathcal{W}_1 \cap \mathcal{W}_2) = m$. Zřejmě platí, že $m \leq k$, $m \leq l$. Vyberme bázi $\{\overrightarrow{u_1}, \dots, \overrightarrow{u_k}\}$ ve $\mathcal{W}_1$, bázi $\{\overrightarrow{v_1}, \dots, \overrightarrow{v_l}\}$ ve $\mathcal{W}_2$ a bázi $\{\overrightarrow{w_1}, \dots, \overrightarrow{w_m}\}$ ve $\mathcal{W}_1 \cap \mathcal{W}_2$. Podle Steinitzovy věty a podle věty 6.15 nyní platí, že po vhodném očíslování $\overrightarrow{u_1}, \dots, \overrightarrow{u_k}$ a $\overrightarrow{v_1}, \dots, \overrightarrow{v_l}$ je množina $\{\overrightarrow{w_1}, \dots, \overrightarrow{w_m}, \overrightarrow{u_{m+1}}, \dots, \overrightarrow{u_k}\}$ bází ve $\mathcal{W}_1$ a množina $\{\overrightarrow{w_1}, \dots, \overrightarrow{w_m}, \overrightarrow{v_{m+1}}, \dots, \overrightarrow{v_l}\}$ je bází ve $\mathcal{W}_2$.

Ukažme, že množina $M = \{\overrightarrow{w_1}, \dots, \overrightarrow{w_m}, \overrightarrow{u_{m+1}}, \dots, \overrightarrow{u_k}, \overrightarrow{v_{m+1}}, \dots, \overrightarrow{v_l}\}$ je bází prostoru $\mathcal{W}_1 + \mathcal{W}_2$.

Nechť $\overrightarrow{z} \in W_1 + W_2$, tedy $\overrightarrow{z} = \overrightarrow{z_1} + \overrightarrow{z_2}$, kde $\overrightarrow{z_1} \in W_1$, $\overrightarrow{z_2} \in W_2$. Potom $\overrightarrow{z_1}$ je lineární kombinací vektorů $\overrightarrow{w_1}, \dots, \overrightarrow{w_m}, \overrightarrow{u_{m+1}}, \dots, \overrightarrow{u_k}$ a vektor $\overrightarrow{z_2}$ je lineární kombinací vektorů $\overrightarrow{w_1}, \dots, \overrightarrow{w_m}, \overrightarrow{v_{m+1}}, \dots, \overrightarrow{v_l}$, a to znamená, že vektor $\overrightarrow{z}$ je lineární kombinací vektorů z množiny $M$.

Stačí proto dokázat, že vektory z množiny $M$ jsou lineárně nezávislé. Předpokládejme, že

$$\sum_{i=1}^{m} c_i \overrightarrow{w_i} + \sum_{j=m+1}^{k} d_j \overrightarrow{u_j} + \sum_{s=m+1}^{l} b_s \overrightarrow{v_s} = \overrightarrow{o}.$$

Pak

$$\sum_{i=1}^{m} c_i \overrightarrow{w_i} + \sum_{j=m+1}^{k} d_j \overrightarrow{u_j} = \sum_{s=m+1}^{l} (-b_s) \overrightarrow{v_s}.$$

Přitom platí, že

$$\sum_{i=1}^{m} c_i \overrightarrow{w_i} + \sum_{j=m+1}^{k} d_j \overrightarrow{u_j} \in W_1,$$

$$\sum_{s=m+1}^{l} (-b_s) \overrightarrow{v_s} \in W_2,$$

a proto vektor

$$\sum_{s=m+1}^{l} (-b_s) \overrightarrow{v_s}$$

patří do $W_1 \cap W_2$. To znamená, že existují $a_1, \dots, a_m \in T$ takové, že

$$\sum_{s=m+1}^{l} (-b_s) \overrightarrow{v_s} = \sum_{i=1}^{m} a_i \overrightarrow{w_i}.$$

Ovšem vektory $\overrightarrow{w_1}, \dots, \overrightarrow{w_m}, \overrightarrow{v_{m+1}}, \dots, \overrightarrow{v_l}$ jsou lineárně nezávislé, proto $a_1 = \ldots = a_m = b_{m+1} = \ldots = b_l = 0$, a tedy

$$\sum_{i=1}^{m} c_i \overrightarrow{w_i} + \sum_{j=m+1}^{k} d_j \overrightarrow{u_j} = \overrightarrow{o}.$$

Z lineární nezávislosti vektorů $\overrightarrow{w_1}, \ldots, \overrightarrow{w_m}, \ldots, \overrightarrow{u_{m+1}}, \ldots, \overrightarrow{u_k}$ odtud plyne, že $c_1 = \ldots = c_m = d_{m+1} = \ldots = d_k = 0$. Proto platí, že vektory $\overrightarrow{w_1}, \ldots, \overrightarrow{w_m}, \overrightarrow{u_{m+1}}, \ldots, \overrightarrow{u_k}, \overrightarrow{v_{m+1}}, \ldots, \overrightarrow{v_l}$ jsou lineárně nezávislé, což znamená, že $M$ je bází podprostoru $\mathcal{W}_1 + \mathcal{W}_2$.

Podle definice dimenze tím dostáváme tvrzení. $\square$

**Věta 6.19** *Je-li vektorový prostor konečné dimenze $\mathcal{V}$ přímým součtem svých podprostorů $\mathcal{W}_1$ a $\mathcal{W}_2$, pak*

$$\dim \mathcal{V} = \dim \mathcal{W}_1 + \dim \mathcal{W}_2.$$

D ů k a z: Tvrzení je přímým důsledkem věty 6.18. $\square$

## 6.3 Cvičení

**6.1** Rozhodněte jsou-li následující vektory vektorového prostoru $\mathcal{R}^4$ mezi sebou lin. závislé nebo lin. nezávislé.

a) $\overrightarrow{a_1} = (1,2,0,0)$, $\overrightarrow{a_2} = (0,1,1,0)$, $\overrightarrow{a_3} = (1,0,0,-1)$, $\overrightarrow{a_4} = (1,1,-1,1)$
b) $\overrightarrow{b_1} = (4,7,1,0)$, $\overrightarrow{b_2} = (2,3,-1,2)$, $\overrightarrow{b_3} = (1,2,1,-1)$, $\overrightarrow{b_4} = (5,7,-4,7)$
c) $\overrightarrow{c_1} = (1,-1,1,2)$, $\overrightarrow{c_2} = (1,8,7,-7)$, $\overrightarrow{c_3} = (1,2,3,-1)$, $\overrightarrow{c_4} = (1,5,5,-4)$
d) $\overrightarrow{d_1} = (2,1,1,1)$, $\overrightarrow{d_2} = (1,2,-1,-2)$, $\overrightarrow{d_3} = (1,-1,-1,1)$, $\overrightarrow{d_4} = (1,2,2,-2)$
e) $\overrightarrow{e_1} = (1,0,1,1)$, $\overrightarrow{e_2} = (0,1,2,3)$, $\overrightarrow{e_3} = (1,2,3,0)$, $\overrightarrow{e_4} = (1,1,0,2)$
f) $\overrightarrow{f_1} = (1,2,-1,1)$, $\overrightarrow{f_2} = (2,-1,4,10)$, $\overrightarrow{f_3} = (1,0,3,-5)$, $\overrightarrow{f_4} = (2,5,2,2)$

[ a), d), e), f) lineárně nezávislé; b),c) lineárně závislé ]

**6.2** Určete všechny hodnoty $\lambda \in \mathbb{R}$, pro které je vektor $\overrightarrow{v}$ lineární kombinací vektorů $\overrightarrow{u_1}$, $\overrightarrow{u_2}$, $\overrightarrow{u_3}$:

a) $\overrightarrow{u_1} = (3,2,5)$, $\overrightarrow{u_2} = (2,4,7)$, $\overrightarrow{u_3} = (5,6,\lambda)$, $\overrightarrow{u_4} = (1,3,5)$
b) $\overrightarrow{u_1} = (4,4,3)$, $\overrightarrow{u_2} = (7,2,1)$, $\overrightarrow{u_3} = (4,1,6)$, $\overrightarrow{u_2} = (5,9,\lambda)$
c) $\overrightarrow{u_1} = (3,2,6)$, $\overrightarrow{u_2} = (7,3,9)$, $\overrightarrow{u_3} = (5,1,3)$, $\overrightarrow{u_3} = (\lambda,2,5)$

[ a) $\lambda \neq 12$; b) $\lambda \in \mathbb{R}$; c) takové $\lambda$ neexistuje ]

**6.3** Zjistěte lineární závislost či nezávislost následujících vektorů prostoru $\mathcal{R}^n$ v závislosti na parametrech.

a) $\overrightarrow{a_1} = (a,b,c,d)$, $\overrightarrow{a_2} = (b,-a,d,-c)$, $\overrightarrow{a_3} = (c,-d,-a,b)$, $\overrightarrow{a_4} = (d,c,-b,-a)$
b) $\overrightarrow{b_1} = (2,3,-1)$, $\overrightarrow{b_2} = (a,4,2)$
c) $\overrightarrow{c_1} = (1,1,1)$, $\overrightarrow{c_2} = (1,a,1)$, $\overrightarrow{c_3} = (2,2,a)$

[ a) $a = b = c = d = 0$ závislé; b) nezávislé; c) $a = 1$, $a = 2$ závislé ]

**6.4** Najděte dimenzi lineárního obalu množin vektorů uvedených v předešlém cvičení v závislosti na parametrech.
[ a) $a = b = c = d = 0$ dimenze 0, jinak 4; b) 2; c) $a = 1$, $a = 2$ dimenze 2, jinak 3 ]

**6.5** Zjistěte dimenzi prostoru $\mathcal{W}_1 \cap \mathcal{W}_2$ jestliže:

a) $\mathcal{W}_1 = [(1,2,0,0),(1,0,0,-1)]$, $\mathcal{W}_2 = [(0,1,1,0),(1,1,-1,1)]$;

b) $\mathcal{W}_1 = [(1,2,3,4)]$, $\mathcal{W}_2 = [(1,5,1,2),(1,1,2,3)]$;

c) $\mathcal{W}_1 = [(1,0,2,-3),(3,2,1,-5),(-1,2,1,-2)]$, $\mathcal{W}_2 = [(-3,0,2,0)]$;

d) $\mathcal{W}_1 = [(3,1,5,4),(2,2,3,3)]$, $\mathcal{W}_2 = [(1,-1,2,1),(1,3,1,2)]$;

e) $\mathcal{W}_1 = [(5,7,-1,3),(1,-3,8,2),(-2,6,-16,-4)]$, $\mathcal{W}_2 = [(9,17,-10,4)]$.

[ a) 0; b) 0; c) 1; d) 2; e) 1 ]

**6.6** Určete dimenzi průniku a součtu podprostorů v $\mathcal{R}^4$ generovaných vektory

$$\overrightarrow{u_1} = (1,1,1,1), \overrightarrow{u_2} = (1,-1,1,-1), \overrightarrow{u_3} = (1,3,1,3)$$

a vektory

$$\overrightarrow{v_1} = (1,2,0,2), \overrightarrow{v_2} = (1,2,1,2), \overrightarrow{v_3} = (3,1,3,1).$$

[ Dimenze průniku je 2, dimenze součtu je 3. ]

**6.7** Uveďte příklad podprostoru $\mathcal{W}$ prostoru $\mathcal{R}^6$, který je přímým součtem dvou podprostorů

a) dimenze 3,

b) dimenze 4,

[ a) např. $[(1,0,0,0,0,0),\ (0,1,0,0,0,0),\ (0,0,1,0,0,0)] \dot{+} [(0,0,0,1,0,0),\ (0,0,0,0,1,0),$ $(0,0,0,0,1,0)]$; b) nelze ]

**6.8** Rozhodněte, je-li podprostorem daného vektorového prostoru množina (není-li uvedeno jinak, vychází vektory z počátku):

a) všechny vektory v rovině, jejichž konce leží na dané přímce;

b) všechny vektory v rovině, jejichž začátky i konce leží na dané přímce;

c) všechny vektory v trojrozměrném prostoru, jejichž konce neleží na dané přímce;

d) všechny vektory v rovině, jejichž konce leží v I. kvadrantu;

e) všech vektorů z $\mathcal{R}^n$, jejichž složky jsou celá čísla;

f) všech vektorů v rovině ležících na souřadnicových osách;

g) všech vektorů $\overrightarrow{u} = (u_1, u_2, \ldots, u_n)$ z $\mathcal{R}^n$, pro které platí $u_1 + u_2 + \ldots + u_n = 0$;

h) všech vektorů $\overrightarrow{u} = (u_1, u_2, \ldots, u_n)$ z $\mathcal{R}^n$, pro které platí $u_1 + u_2 + \ldots + u_n = 5$.
[ a) ano, prochází-li přímka počátkem; b) ano; c),d) ne; e), f), h) ne; g) ano ]

**6.9** Nechť $\mathcal{W}_1 = [\{\overrightarrow{u_1}, \overrightarrow{u_2}, \overrightarrow{u_3}\}]$, $\mathcal{W}_2 = [\{\overrightarrow{v_1}, \overrightarrow{v_2}, \overrightarrow{v_3}\}]$ jsou podprostory v $\mathcal{R}^4$ takové, že

$$\overrightarrow{u_1} = (1,2,1,-2), \overrightarrow{u_2} = (2,3,1,0), \overrightarrow{u_3} = (1,2,2,-3),$$

$$\overrightarrow{v_1} = (1,1,1,1), \overrightarrow{v_2} = (1,0,1,-1), \overrightarrow{v_3} = (1,3,0,-4).$$

Najděte některou bázi prostoru $\mathcal{W}_1 \dot{+} \mathcal{W}_2$.
[ např. $\{\overrightarrow{u_1}, \overrightarrow{u_2}, \overrightarrow{u_3}, \overrightarrow{v_2}\}$ ]

# Kapitola 7

# Soustavy lineárních rovnic

## 7.1 Elementární transformace

Také v této části bude $\mathcal{T}$ označovat číselné těleso. Pokud je $A = ||a_{ik}||$ matice nad $\mathcal{T}$ typu $m \times n$, pak řádky matice $A$ budeme považovat za vektory aritmetického vektorového prostoru $\mathcal{T}^n$.

**Definice 7.1** Řádkovým podprostorem určeným maticí $A$ *budeme rozumět podprostor v* $\mathcal{T}^n$ *generovaný řádky matice* $A$.

**Definice 7.2** *Elementárními řádkovými transformacemi matice* $A$ *nazýváme následující operace:*

1. *výměna libovolných dvou řádků v* $A$*;*

2. *vynásobení některého řádku v* $A$ *prvkem z* $\mathcal{T}$ *různým od nuly;*

3. *přičtení libovolného násobku některého řádku z* $A$ *k jinému řádku v* $A$.

**Definice 7.3** *Jsou-li* $A, B \in M_{m \times n}(\mathcal{T})$*, pak řekneme, že matice* $B$ *je* řádkově ekvivalentní s maticí $A$ *(značíme* $A \overset{\check{r}}{\sim} B$*), může-li* $B$ *vzniknout z* $A$ *pomocí konečného počtu elementárních řádkových transformací.*

Poznámka: Je zřejmé, že jsou-li $A, B, C \in M_{m \times n}(\mathcal{T})$, pak platí

a) $A \overset{\check{r}}{\sim} A$,

b) $A \overset{\check{r}}{\sim} B \Longrightarrow B \overset{\check{r}}{\sim} A$,

c) $(A \overset{\check{r}}{\sim} B \wedge B \overset{\check{r}}{\sim} C) \Longrightarrow A \overset{\check{r}}{\sim} C$.

Můžeme proto mj. v případě $A \overset{\check{r}}{\sim} B$ říkat, že matice $A$ a $B$ *jsou řádkově ekvivalentní.*

**Věta 7.1** *Jsou-li* $A, B \in M_{m \times n}(\mathcal{T})$ *takové, že* $A \overset{\check{r}}{\sim} B$*, pak matice* $A$ *a* $B$ *určují stejné řádkové podprostory v* $\mathcal{T}^n$*.*

D ů k a z: Zřejmě stačí dokázat, že použitím kterékoliv elementární řádkové transformace dostaneme matici, která určuje stejný řádkový podprostor jako původní matice. Připomeňme si, že řádkový podprostor $[\{\overrightarrow{a_1}, \ldots, \overrightarrow{a_m}\}]$ určený maticí

$$A = \begin{Vmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{a_m} \end{Vmatrix}$$

se skládá právě ze všech vektorů z $\mathcal{T}^n$, které jsou ve tvaru

$$\sum_{i=1}^{m} c_i \overrightarrow{a_i},$$

kde $c_1, \ldots, c_m$ jsou libovolná čísla z $T$. Přitom provedení elementární řádkové transformace na matici $A$ znamená v jednotlivých případech

1. výměnu vektoru $\overrightarrow{a_i}$ s vektorem $\overrightarrow{a_j}$ $\quad (i \neq j)$,
2. nahrazení vektoru $\overrightarrow{a_i}$ vektorem $c\overrightarrow{a_i}$ $\quad (0 \neq c \in T)$,
3. nahrazení vektoru $\overrightarrow{a_j}$ vektorem $\overrightarrow{a_j} + d\overrightarrow{a_i}$ $\quad (i \neq j, d \in T)$.

V 1. případě je zřejmé, že se řádkový podprostor nezmění, protože sčítání vektorů je komutativní.

Ve 2. případě máme ověřit, že se sobě rovnají řádkové podprostory určené maticemi

$$A = \begin{Vmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{a_i} \\ \vdots \\ \overrightarrow{a_m} \end{Vmatrix} \quad \text{a} \quad A_1 = \begin{Vmatrix} \overrightarrow{a_1} \\ \vdots \\ c\overrightarrow{a_i} \\ \vdots \\ \overrightarrow{a_m} \end{Vmatrix}.$$

Je-li

$$\overrightarrow{u} = \sum_{k=1}^{m} c_k \overrightarrow{a_k},$$

pak $\overrightarrow{u} = c_1\overrightarrow{a_1} + \ldots + \frac{c_i}{c}(c\overrightarrow{a_i}) + \ldots + c_m\overrightarrow{a_m}$, tedy

$$[\{\overrightarrow{a_1}, \ldots, \overrightarrow{a_i}, \ldots, \overrightarrow{a_m}\}] \subseteq\subseteq [\{\overrightarrow{a_1}, \ldots, c\overrightarrow{a_i}, \ldots, \overrightarrow{a_m}\}].$$

Obráceně, platí-li

$$\overrightarrow{v} = d_1\overrightarrow{a_1} + \ldots + d_i(c\overrightarrow{a_i}) + \ldots + d_m\overrightarrow{a_m},$$

pak můžeme psát

$$\overrightarrow{v} = d_1\overrightarrow{a_1} + \ldots + (d_i c)\overrightarrow{a_i} + \ldots + d_m\overrightarrow{a_m},$$

a tedy

$$[\{\overrightarrow{a_1}, \dots, c\overrightarrow{a_i}, \dots, \overrightarrow{a_m}\}] \subseteq\subseteq [\{\overrightarrow{a_1}, \dots, \overrightarrow{a_i}, \dots, \overrightarrow{a_m}\}].$$

To ovšem znamená, že

$$[\{\overrightarrow{a_1}, \dots, \overrightarrow{a_i}, \dots, \overrightarrow{a_m}\}] = [\{\overrightarrow{a_1}, \dots, c\overrightarrow{a_i}, \dots, \overrightarrow{a_m}\}].$$

Ve 3. případě budeme uvažovat řádkové podprostory určené maticemi

$$A = \left\| \begin{matrix} \overrightarrow{a_1} \\ \overrightarrow{a_2} \\ \vdots \\ \overrightarrow{a_m} \end{matrix} \right\| \quad \text{a} \quad B = \left\| \begin{matrix} \overrightarrow{a_1} + d\overrightarrow{a_2} \\ \overrightarrow{a_2} \\ \vdots \\ \overrightarrow{a_m} \end{matrix} \right\|.$$

(Bez újmy na obecnosti můžeme uvažovat tento případ, kdy k prvnímu řádku přičítáme násobek druhého řádku; jinak bychom mohli pomocí transformací typu 1 řádky zaměnit.)

Nechť

$$\overrightarrow{u} = \sum_{k=1}^{m} c_k \overrightarrow{a_k}.$$

Pak platí

$$\overrightarrow{u} = c_1(\overrightarrow{a_1} + d\overrightarrow{a_2}) + (-c_1 d + c_2)\overrightarrow{a_2} + c_3\overrightarrow{a_3} + \dots + c_m\overrightarrow{a_m},$$

proto

$$[\{\overrightarrow{a_1}, \overrightarrow{a_2}, \dots, \overrightarrow{a_m}\}] \subseteq\subseteq [\{\overrightarrow{a_1} + d\overrightarrow{a_2}, \overrightarrow{a_2}, \dots, \overrightarrow{a_m}\}].$$

Obráceně, nechť

$$\overrightarrow{v} = d_1(\overrightarrow{a_1} + d\overrightarrow{a_2}) + \sum_{i=2}^{m} d_i \overrightarrow{a_i}.$$

Pak $\overrightarrow{v} = d_1\overrightarrow{a_1} + (d + d_2)\overrightarrow{a_2} + d_3\overrightarrow{a_3} + \dots + d_m\overrightarrow{a_m}$, tedy

$$[\{\overrightarrow{a_1} + d\overrightarrow{a_2}, \overrightarrow{a_2}, \dots, \overrightarrow{a_m}\}] \subseteq\subseteq [\{\overrightarrow{a_1}, \overrightarrow{a_2}, \dots, \overrightarrow{a_m}\}].$$

Platí proto, že řádkové podprostory určené maticemi $A$ a $B$ se sobě rovnají. $\square$

**Definice 7.4** *Je-li $A \in M_{m\times n}(\mathcal{T})$, pak* vedoucím prvkem *nenulového řádku $\overrightarrow{a_i}$ matice $A$ rozumíme první nenulový prvek v $\overrightarrow{a_i}$.*

**Definice 7.5** *Řekneme, že matice $A$ je* redukovaná, *je-li vedoucí prvek každého nenulového řádku v $A$ roven 1 a jestliže v každém sloupci matice $A$, který obsahuje vedoucí prvek některého řádku, jsou všechny zbývající prvky rovny 0.*

**Příklad 7.1** Matice

$$\begin{pmatrix} 0 & 0 & 1 & 2 & -1 & 3 \\ 1 & 0 & 0 & 3 & 6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 5 & 2 & -4 \end{pmatrix}$$

je redukovaná.

**Věta 7.2** *Každá matice $A$ je řádkově ekvivalentní s některou redukovanou maticí, kterou můžeme získat z $A$ pomocí elementárních řádkových transformací typu 2 a 3.*

D ů k a z: Nechť $A = ||a_{ij}|| \in M_{m\times n}(\mathcal{T})$. Předpokládejme, že první řádek v $A$ je nenulový a že jeho vedoucí prvek je $a_{1k}$. (Pokud by byl první řádek nulový, prováděli bychom následující úvahy analogickým způsobem s prvním nenulovým řádkem.) Vynásobením řádku $\overrightarrow{a_1}$ prvkem $a_{1k}^{-1}$ bude vedoucí prvek prvního řádku roven 1. Nyní pro každé $i \neq 1$ přičteme k $i$-tému řádku $(-a_{ik})$-tý násobek prvního řádku. Dostaneme tak v $k$-tém sloupci s výjimkou prvního prvku všechny zbývající prvky rovny nule. Analogický postup pak provádíme s ostatními nenulovými řádky. Ve výsledku dostaneme redukovanou matici, která je s původní maticí $A$ vskutku řádkově ekvivalentní. □

`Poznámka`: Pokud navíc použijeme ještě transformace typu 1, můžeme od libovolné matice přejít k matici následujícího tvaru:

a) všechny nulové řádky jsou umístěny až za všemi nenulovými řádky;

b) jsou-li $\overrightarrow{a_i}, \overrightarrow{a_j}$, $i < j$, nenulové řádky, které mají své vedoucí prvky ve sloupcích $k_i, k_j$, pak $k_i < k_j$.

**Definice 7.6** *Redukovanou matici, která splňuje podmínky* a) *a* b), *nazýváme* redukovaná trojúhelníková matice.

**Příklad 7.2** Redukovanou trojúhelníkovou maticí je matice

$$\begin{pmatrix} 1 & 0 & 0 & 3 & -2 \\ 0 & 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

zatímco redukovaná matice z příkladu 7.1 není trojúhelníková.

Platí:

**Věta 7.3** *Každá matice je řádkově ekvivalentní s některou redukovanou trojúhelníkovou maticí.* □

**Věta 7.4** *Nechť $A \in M_{m\times n}(\mathcal{T})$ je redukovaná matice s nenulovými řádky $\overrightarrow{a_1}, \dots, \overrightarrow{a_r}$, které mají vedoucí prvky ve sloupcích $k_1, \dots, k_r$. Potom pro každý vektor*

$$\overrightarrow{u} = \sum_{i=1}^{r} c_i \overrightarrow{a_i}$$

*řádkového podprostoru určeného maticí $A$ platí, že koeficient $c_i$ je roven $k_i$-té souřadnici vektoru $\overrightarrow{u}$.*

D ů k a z: V $k_i$-tém sloupci jsou podle definice redukované matice všechny prvky s výjimkou $i$-tého místa rovny 0 a na $i$-tém místě je číslo 1. Odtud přímo dostáváme tvrzení. □

**Věta 7.5** *Nenulové řádky redukované matice jsou lineárně nezávislé.*

D ů k a z: Tvrzení je důsledkem věty 7.4. □

**Věta 7.6** *Je-li matice $A$ řádkově ekvivalentní s redukovanou maticí $B$, pak nenulové řádky matice $B$ tvoří bázi řádkového podprostoru určeného maticí $A$.*

D ů k a z: Věta je důsledkem věty 7.5 a 7.1. □

## 7.2 Hodnosti matic

**Definice 7.7** Hodností matice $A \in M_{m\times n}(\mathcal{T})$ *rozumíme dimenzi řádkového podprostoru v $\mathcal{T}^n$ určeného maticí $A$. (Hodnost matice $A$ budeme značit $h(A)$.)*

`Poznámka:`

a) Podle definice řádkového podprostoru určeného maticí $A$ je zřejmé, že hodnost matice $A$ je rovna maximálnímu počtu jejích lineárně nezávislých řádků. Mj. tedy platí $h(A) \leq m$.

b) Řádkově ekvivalentní matice mají stejnou hodnost.

c) Hodnost matice $A$ je rovna počtu nenulových řádků libovolné trojúhelníkové matice, která je řádkově ekvivalentní s $A$.

**Definice 7.8** *Je-li $A \in M_{m\times n}(\mathcal{T})$, pak* subdeterminantem $k$-tého stupně *matice $A$ (kde $k \leq min(m,n)$) rozumíme determinant libovolné čtvercové matice $k$-tého stupně, která vznikne z prvků matice $A$ ležících na průsečících daných $k$ řádku a $k$ sloupců.*

**Příklad 7.3** Pro matici

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

jsou jejími subdeterminanty 2.stupně např. determinanty

$$\begin{vmatrix} 5 & 2 \\ -2 & 3 \end{vmatrix} = 19 \qquad \begin{vmatrix} 2 & 0 \\ -8 & 9 \end{vmatrix} = 18$$

a subdeterminantem 3, stupně např. determinant

$$\begin{vmatrix} 5 & 2 & 0 \\ -2 & 3 & -1 \\ 6 & -8 & 9 \end{vmatrix} = 119.$$

**Věta 7.7** *Hodnost matice $A$ je rovna maximálnímu stupni nenulového subdeterminantu matice $A$.*

D ů k a z: Uvažujme matici

$$A = \left\| \begin{vmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{a_n} \end{vmatrix} \right\| \in M_{m\times n}(\mathcal{T}).$$

a) Předpokládejme, že maximální stupeň nenulového subdeterminantu matice $A$ je roven $h$ a determinant

$$\mathcal{A}_h = \begin{vmatrix} a_{11} & \cdots & a_{1h} \\ \vdots & \ddots & \vdots \\ a_{h1} & \cdots & a_{hh} \end{vmatrix} \neq 0.$$

(Předpoklad nenulovosti právě subdeterminantu $\mathcal{A}_h$ není na úkor obecnosti, protože záměny řádků a sloupců mají vliv jenom na znaménko determinantu, ale ne na jeho nulovost.)
Dokážeme, že

$$[\{\overrightarrow{a_1}, \dots, \overrightarrow{a_m}\}] = [\{\overrightarrow{a_1}, \dots, \overrightarrow{a_h}\}].$$

Uvažujeme libovolný řádek $\overrightarrow{a_i}$, kde $i = h+1, \dots, m$. Je-li $j = h+1, \dots, n$, potom podle předpokladu platí

$$A = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1h} & a_{1j} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{h1} & a_{h2} & \cdots & a_{hh} & a_{hj} \\ a_{i1} & a_{i2} & \cdots & a_{ih} & a_{ij} \end{vmatrix} = 0.$$

Tato rovnost platí i pro každé $j = 1, \dots, h$, protože se pak jedná o determinant matice, která má stejné dva sloupce. Pomocí Laplaceovy věty (rozvinutím podle posledního sloupce) můžeme získanou rovnost zapsat ve tvaru

$$a_{1j}\mathcal{B}_1 + a_{2j}\mathcal{B}_2 + \cdots + a_{hj}\mathcal{B}_h + a_{ij}\mathcal{A}_h = 0.$$

Přitom pro každé $j = 1, \dots, n$ dostáváme stejné prvky $\mathcal{B}_1, \dots, \mathcal{B}_h, \mathcal{A}_h$. Proto můžeme těchto $n$ rovností přepsat vektorově (přejdeme-li od transponovaných vektorů k řádkovým vektorům matice $A$) ve tvaru rovnosti

$$\mathcal{B}_1\overrightarrow{a_1} + \mathcal{B}_2\overrightarrow{a_2} + \cdots + \mathcal{B}_h\overrightarrow{a_h} + \mathcal{A}_h\overrightarrow{a_i} = \overrightarrow{o}.$$

Tedy

$$\overrightarrow{a_i} = -\frac{\mathcal{B}_1}{\mathcal{A}_h}\overrightarrow{a_1} - \frac{\mathcal{B}_2}{\mathcal{A}_h}\overrightarrow{a_2} - \cdots - \frac{\mathcal{B}_h}{\mathcal{A}_h}\overrightarrow{a_h},$$

což znamená, že $\overrightarrow{a_i}$ je lineární kombinací vektorů $\overrightarrow{a_1}, \dots, \overrightarrow{a_h}$ $(i = h+1, \dots, m)$. Proto opravdu platí

$$[\{\overrightarrow{a_1}, \dots, \overrightarrow{a_m}\}] = [\{\overrightarrow{a_1}, \dots, \overrightarrow{a_h}\}].$$

Zbývá dokázat, že řádky $\overrightarrow{a_1}, \dots, \overrightarrow{a_h}$ jsou lineárně nezávislé. Dokažme obecně, že je-li

$$B = \left\| \begin{matrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{matrix} \right\| = \left\| \begin{matrix} \overrightarrow{b_1} \\ \vdots \\ \overrightarrow{b_n} \end{matrix} \right\| \in M_n(\mathcal{T}),$$

pak $\det B = 0$ právě tehdy, když $\overrightarrow{b_1}, \dots, \overrightarrow{b_h}$ jsou lineárně závislé. Dokážeme implikaci „$\Longrightarrow$“. (Implikaci „$\Longleftarrow$“ jsme již dokázali ve větě 5.21.)
Nechť $\det B = 0$. Je-li $B$ nulová matice, pak jsou její řádky samozřejmě lineárně závislé. Nechť tedy v $B$ existuje nenulový subdeterminant stupně $h \geq 1$ a nechť všechny subdeterminanty stupňů vyšších než $h$ jsou rovny nule. Předpokládejme, že

$$\begin{vmatrix} b_{11} & \cdots & b_{1h} \\ \vdots & \ddots & \vdots \\ b_{h1} & \cdots & b_{hh} \end{vmatrix} \neq 0.$$

Podle předchozí části důkazu pak platí

$$[\{\overrightarrow{b_1}, \dots, \overrightarrow{b_n}\}] = [\{\overrightarrow{b_1}, \dots, \overrightarrow{b_h}\}],$$

a protože $h < n$, jsou vektory $\overrightarrow{b_1}, \dots, \overrightarrow{b_n}$ lineárně závislé.
Vrátíme-li se tedy k původní matici $A$, pak na základě předpokladu $\mathcal{A}_h \neq 0$ dostáváme, že vektory $\overrightarrow{a_1}, \dots, \overrightarrow{a_h}$ jsou lineárně nezávislé. Proto $\dim[\{\overrightarrow{a_1}, \dots, \overrightarrow{a_m}\}] = h$, tedy také $h(A) = h$.

b) Nechť $h(A) = h$, tj. $\dim[\{\overrightarrow{a_1}, \dots, \overrightarrow{a_m}\}] = h$. Pak pro každých $h' > h$ řádků matice $A$ platí, že tyto řádky jsou lineárně závislé, a proto podle věty 5.21 jsou všechny subdeterminanty stupně $h'$ rovny 0. Přitom však alespoň jeden subdeterminant matice $A$ stupně $h$ musí být nenulový, protože jinak by podle části a) důkazu platilo, že $\dim[\{\overrightarrow{a_1}, \dots, \overrightarrow{a_m}\}] < h$. □

**Věta 7.8** *Hodnost matice $A$ je rovna maximálnímu počtu lineárně nezávislých sloupců matice $A$.*

D ů k a z: Tvrzení vyplývá z poznámky za definicí 7.7 (část a)), ze skutečnosti, že determinant čtvercové matice je roven determinantu matice transponované a z věty 7.7.□

`Poznámka:` Na základě důkazu věty 7.7 můžeme vypočítat hodnost matice $A$ také následujícím způsobem, který se nazývá také „metoda vroubení minorů“:

Nechť je dána nenulová matice $A \in M_{m\times n}(\mathcal{T})$. Protože existuje alespoň jeden její nenulový prvek, platí $h(A) \geq 1$. Zvolme si jeden z těchto nenulových prvků. Uvažujme nyní všechny subdeterminanty 2. stupně matice $A$, které obsahují zvolený prvek. Jsou-li všechny tyto subdeterminanty rovny 0, pak $h(A) = 1$, v opačném případě $h(A) \geq 2$. V druhém z případů vybereme jeden z uvažovaných nenulových subdeterminantů a počítáme subdeterminanty 3. stupně, které obsahují tento vybraný subdeterminant 2. stupně. Pokud je alespoň jeden z těchto subdeterminantů 3. stupně nenulový, pak $h(A) \geq 3$, jinak je $h(A) = 2$.

Takto postupujeme do té doby, dokud nedostaneme nenulový subdeterminant $h$-tého stupně takový, že buď všechny subdeterminanty $(h+1)$-ho stupně, které jej obsahují, jsou rovny 0, nebo $h = \min\{m, n\}$. Pak platí $h(A) = h$.

**Příklad 7.4** Určete hodnost matice

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

.

a) Nejdříve vypočítáme $h(A)$ pomocí elementárních řádkových transformací. Platí

$$A \overset{\check{r}}{\sim} \begin{pmatrix} 2 & 3 & -2 & 1 \\ 0 & -4 & 5 & -5 \\ 0 & 8 & -10 & 10 \end{pmatrix} \overset{\check{r}}{\sim} \begin{pmatrix} 2 & 3 & -2 & 1 \\ 0 & -4 & 5 & -5 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Je zřejmé, že poslední matice má hodnost rovnu 2, proto také $h(A) = 2$.
(Pro určení hodnosti stačilo převést matici $A$ na tvar, který se liší od redukovaného tvaru tím, že vedoucí prvky nenulových řádků mohou být různé od 1.)

b) Určíme $h(A)$ vroubením subdeterminantů (minorů). Vybereme si např. prvek 2 na průsečíku 1. řádku a 1. sloupce. Ten je vrouben nenulovým subdeterminantem 2. stupně

$$\mathcal{A}_2 = \begin{vmatrix} 2 & 3 \\ 4 & 2 \end{vmatrix} = -8,$$

tedy $h(A) \geq 2$. Subdeterminant $\mathcal{A}_2$ je vrouben subdeterminanty 3. stupně

$$\begin{vmatrix} 2 & 3 & -2 \\ 4 & 2 & 1 \\ -2 & 5 & -8 \end{vmatrix} \quad \text{a} \quad \begin{vmatrix} 2 & 3 & 1 \\ 4 & 2 & -3 \\ -2 & 5 & 9 \end{vmatrix}.$$

Protože jsou oba tyto subdeterminanty rovny 0, platí $h(A) = 2$.

## 7.3 Řešení soustav lineárních rovnic

**Definice 7.9** *Je-li $\mathcal{T}$ číselné těleso, pak* lineárním polynomem *o $n$ proměnných nad $\mathcal{T}$ rozumíme každé zobrazení $f : T^n \longrightarrow T$ takové, že*

$$f(x_1, \ldots, x_n) = a_1x_1 + \ldots + a_nx_n = \sum_{i=1}^{n} a_ix_i,$$

*kde $a_1, \ldots, a_n \in \mathcal{T}$.*

**Definice 7.10** *Nechť*

$$\sum_{i=1}^{n} a_ix_i$$

*je lineární polynom nad tělesem $\mathcal{T}$, $b \in T$. Potom úloha určit všechny uspořádané $n$-tice $(\xi_1, \ldots, \xi_n) \in T^n$, pro které platí*

$$\sum_{i=1}^{n} a_i\xi_i = b,$$

*se nazývá* lineární rovnice o $n$ neznámých nad $\mathcal{T}$.

*Každá $n$-tice $(\xi_1, \ldots, \xi_n) \in T^n$, pro kterou nastane rovnost*

$$\sum_{i=1}^{n} a_i\xi_i = b,$$

*se nazývá* řešení *této rovnice.*

**Definice 7.11** *Nechť*

$$\sum_{i=1}^{n} a_{1i}x_i, \ldots, \sum_{i=1}^{n} a_{mi}x_i$$

*jsou lineární polynomy nad* $\mathcal{T}$, $b_1, \ldots, b_m \in T$. *Pak úloha určit všechny uspořádané* $n$*-tice*

$$(\xi_1, \ldots, \xi_n) \in T^n,$$

*pro které platí*

$$(S) \begin{cases} \sum_{i=1}^{n} a_{1i}\xi_i = b_1 & (R_1) \\ \ldots\ldots\ldots\ldots & \\ \sum_{i=1}^{n} a_{mi}\xi_i = b_m & (R_m) \end{cases}$$

*se nazývá* soustava $m$ lineárních rovnic o $n$ neznámých nad $\mathcal{T}$.

*Pokud platí* $b_i = 0$ *pro každé* $i = 1, \ldots, m$, *pak se soustava nazývá* homogenní, *v opačném případě se nazývá* nehomogenní.

`Poznámka:` Jsou-li $M_1, \ldots, M_m \subseteq T^n$ množiny řešení rovnic $(R_1), \ldots, (R_m)$, pak pro množinu $M$ řešení soustavy $(S)$ platí

$$M = \bigcap_{j=1}^{m} M_j.$$

**Definice 7.12** *Je-li (S) soustava lineárních rovnic z definice 7.11, potom matici*

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

*nazýváme* maticí soustavy *(S), resp.* rozšířenou maticí soustavy *(S).*

`Poznámka:`

a) Soustava (S) je jednoznačně určena (až na označení neznámých) pomocí své rozšířené matice.

b) Řádky rozšířené matice jsou vektory z aritmetického vektorového prostoru $\mathcal{T}^{n+1}$, proto i pro rovnice budeme používat terminologii, která se týká vektorů. (Např. budeme hovořit o lineární kombinaci rovnic, apod.)

c) Označíme-li

$$\overrightarrow{\xi}^T = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} \quad \text{a} \quad \overrightarrow{b}^T = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix},$$

pak soustavu (S) můžeme maticově zapsat ve tvaru

$$A\overrightarrow{\xi}^T = \overrightarrow{b}^T.$$

Řešením této soustavy pak bude každý vektor $\overrightarrow{u} \in T^n$, pro který platí $A\overrightarrow{u}^T = \overrightarrow{b}^T$.

Pro označení rozšířené matice soustavy (S) budeme také používat symbolu $(A, \overrightarrow{b}^T)$.

**Definice 7.13** *Dvě soustavy lineárních rovnic o $n$ neznámých $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$ a $B\overrightarrow{\eta}^T = \overrightarrow{c}^T$ nad $\mathcal{T}$ se nazývají* ekvivalentní, *mají-li stejné množiny řešení.*

**Definice 7.14** *Soustava lineárních rovnic $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$ nad $\mathcal{T}$ se nazývá* řešitelná, *existuje-li alespoň jedno její řešení.*

**Věta 7.9** *Nehomogenní soustava lineárních rovnic $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$ je řešitelná právě tehdy, je-li vektor $\overrightarrow{b}^T$ lineární kombinací sloupců matice $A$.*

D ů k a z: Nechť $A = ||\overrightarrow{d_1}^T, \dots, \overrightarrow{d_n}^T||$. Zřejmě pak můžeme soustavu $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$ zapsat ve tvaru

$$\sum_{i=1}^{n} \xi_1 \overrightarrow{d_i}^T = \overrightarrow{b}^T.$$

Tedy je-li daná soustava řešitelná, pak existují $\xi_1, \dots, \xi_n$, která vyhovují poslední rovnosti, a proto je $\overrightarrow{b}^T$ lineární kombinací vektorů $\overrightarrow{d_1}^T, \dots, \overrightarrow{d_n}^T$ s koeficienty $\xi_1, \dots, \xi_n$. Je-li naopak $\overrightarrow{b}^T$ lineární kombinací vektorů $\overrightarrow{d_1}^T, \dots, \overrightarrow{d_n}^T$, pak koeficienty této lineární kombinace jsou složkami vektoru, který je řešením dané soustavy. □

**Věta 7.10 (Frobeniova věta)** *Nehomogenní soustava lineárních rovnic $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$ je řešitelná tehdy a jen tehdy, platí-li $h(A) = h((A, \overrightarrow{b}^T))$.*

D ů k a z: Podle věty 7.8 víme, že hodnost matice je rovna maximálnímu počtu lineárně nezávislých sloupců této matice, jinými slovy, hodnost matice typu $m \times n$ je dimenze podprostoru v $T^m$ generovaného sloupcovými vektory té matice.

Nechť $A = ||\overrightarrow{d_1}^T, \dots, \overrightarrow{d_n}^T||$ a nechť je soustava $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$ řešitelná. Potom podle předchozí věty platí $\overrightarrow{b}^T \in [\{\overrightarrow{d_1}^T, \dots, \overrightarrow{d_n}^T\}]$. To ovšem znamená, že

$$h(A) = \dim[\{\overrightarrow{d_1}^T, \dots, \overrightarrow{d_n}^T\}] = \dim[\{\overrightarrow{d_1}^T, \dots, \overrightarrow{d_n}^T, \overrightarrow{b}^T\}] = h((A, \overrightarrow{b}^T)).$$

Obráceně, předpokládejme, že $h(A) = h((A, \overrightarrow{b}^T))$, tj.

$$\dim[\{\overrightarrow{d_1}^T, \dots, \overrightarrow{d_n}^T\}] = \dim[\{\overrightarrow{d_1}^T, \dots, \overrightarrow{d_n}^T, \overrightarrow{b}^T\}].$$

Přitom ale platí, že

$$[\{\overrightarrow{d_1}^T, \dots, \overrightarrow{d_n}^T\}] \subseteq\subseteq [\{\overrightarrow{d_1}^T, \dots, \overrightarrow{d_n}^T, \overrightarrow{b}^T\}],$$

proto podle věty 6.17 platí

$$[\{\overrightarrow{d_1}^T, \dots, \overrightarrow{d_n}^T\}] = [\{\overrightarrow{d_1}^T, \dots, \overrightarrow{d_n}^T, \overrightarrow{b}^T\}].$$

To ovšem znamená, že

$$\overrightarrow{b}^T \in [\{\overrightarrow{d_1}^T, \dots, \overrightarrow{d_n}^T\}],$$

a proto podle věty 7.9 je daná soustava řešitelná. □

**Věta 7.11** *Jsou-li* $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$ *a* $B\overrightarrow{\xi}^T = \overrightarrow{c}^T$ *dvě soustavy (nehomogenních) lineárních rovnic o* $n$ *neznámých nad* $\mathcal{T}$ *takové, že jejich rozšířené matice* $(A, \overrightarrow{b}^T)$ *a* $(B, \overrightarrow{c}^T)$ *jsou řádkově ekvivalentní, pak jsou tyto soustavy ekvivalentní.*

D ů k a z: Připomeňme, že dvě matice jsou řádkově ekvivalentní, je-li možno přejít od jedné z nich k druhé pomocí konečného počtu elementárních řádkových transformací. Proto stačí ověřit tvrzení pro takové soustavy rovnic, u kterých se jejich rozšířené matice liší o jedinou elementární řádkovou transformaci.

a) Nechť $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$ je soustava $m$ lineárních rovnic o $n$ neznámých. Je zřejmé, že záměnou dvou řádků v matici $(A, \overrightarrow{b}^T)$ dostaneme rozšířenou matici soustavy ekvivalentní s původní soustavou, protože množina řešení každé soustavy rovnic je průnikem množin řešení jednotlivých rovnic.

b) Vynásobíme-li např. $k$-tý řádek ($k \in \{1, \ldots, m\}$) matice $(A, \overrightarrow{b}^T)$ nenulovým prvkem $c \in T$, je získaná matice rozšířenou maticí soustavy rovnic, která se liší od soustavy $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$ jenom tím, že místo $k$-té rovnice

$$\sum_{i=1}^{n} a_{ki}\xi_i = b_k$$

původní soustavy je její $k$-tá rovnice ve tvaru

$$c\sum_{i=1}^{n} a_{ki}\xi_i = cb_k.$$

Ovšem množiny řešení těchto dvou rovnic jsou stejné. Proto vzhledem k tomu, že ostatní rovnice obou soustav se sobě rovnají, jsou tyto soustavy rovnic ekvivalentní.

c) Konečně předpokládejme, že jsme ke $k$-tému řádku matice $(A, \overrightarrow{b}^T)$ přičetli $d$-násobek $j$-tého řádku této matice ($k \neq j$). Vzniklá matice je maticí soustavy $(S')$ rovnic, která se liší od soustavy $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$ jenom v $k$-té rovnici. (Původní soustava má $k$-tou rovnici

$$\sum_{i=1}^{n} a_{ki}\xi_i = b_k,$$

zatímco v nové soustavě je to rovnice

$$\sum_{i=1}^{n} a_{ki}\xi_i + d\sum_{i=1}^{n} a_{ji}\xi_i = b_k + db_j.)$$

Nechť $\overrightarrow{u} = (u_1, \ldots, u_n)$ je řešením soustavy $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$. Pak platí

$$\sum_{i=1}^{n} a_{pi}u_i = b_p$$

pro každé $p = 1, \dots, m$, proto platí také

$$\sum_{i=1}^{n} a_{ki}u_i + d\sum_{i=1}^{n} a_{ji}u_i = b_k + db_j,$$

tedy $\overrightarrow{u}$ je řešením soustavy $(S^T)$.
Předpokládejme obráceně, že $\overrightarrow{v} = (v_1, \dots, v_n)$ je řešením soustavy $(S')$. Protože obecně platí

$$\sum_{i=1}^{n} a_{ki}\xi_i = \left(\sum_{i=1}^{n} a_{ki}\xi_i + d\sum_{i=1}^{n} a_{ji}\xi_i\right) - d\sum_{i=1}^{n} a_{ji}\xi_i$$

a protože podle předpokladu

$$\sum_{i=1}^{n} a_{ki}v_i + d\sum_{i=1}^{n} a_{ji}v_i = b_k + db_j \quad \text{a} \quad d\sum_{i=1}^{n} a_{ji}v_i = db_j,$$

platí také

$$\sum_{i=1}^{n} a_{ki}v_i = \left(\sum_{i=1}^{n} a_{ki}v_i + d\sum_{i=1}^{n} a_{ji}v_i\right) - d\sum_{i=1}^{n} a_{ji}v_i = (b_k + db_j) - db_j = b_k,$$

tedy $\overrightarrow{v}$ je řešením rovnice

$$\sum_{i=1}^{n} a_{ki}\xi_i = b_k.$$

Protože všechny ostatní rovnice obou soustav jsou stejné, je $\overrightarrow{v}$ řešením soustavy $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$.

□

`Poznámka:`

a) Právě dokázaná věta platí samozřejmě i pro homogenní soustavy lineárních rovnic, protože pravé strany všech jejich rovnic zůstávají při všech transformacích nulové. Můžeme zde navíc pravé strany v úvahách vynechat a místo rozšířené matice používat matici soustavy.

b) Z každé soustavy můžeme vypustit každou rovnici tvaru $0 = 0$, protože její množinou řešení je $T^n$.

c) Na základě věty 7.11 je založena také metoda řešení soustav lineárních rovnic zvaná *Gaussova eliminační metoda*. Popíšeme si ji podrobněji:
Nechť $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$ je soustava $m$ lineárních rovnic o $n$ neznámých, jejíž rozšířená matice je

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

Předpokládejme, že $a_{11} \neq 0$. (Pokud by tomu tak nebylo, můžeme toho dosáhnout podle věty 7.11 záměnou řádků.) Pro každé $k = 2, \dots, m$ přičteme ke $k$-tému řádku matice $(-\frac{a_{k1}}{a_{11}})$-násobek 1. řádku této matice. Ve vzniklé matici jsou všechny prvky 1. sloupce s výjimkou 1. řádku rovny nule. Podle části b) můžeme vynechat všechny eventuální řádky obsahující samé nuly. Výsledná matice je potom ve tvaru

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ 0 & a'_{22} & \cdots & a'_{2n} & b'_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & a'_{r2} & \cdots & a'_{rn} & b'_r \end{array}\right),$$

kde $r \leq m$.

Předpokládejme, že $a'_{22} \neq 0$. (Jestliže tomu tak není a je-li alespoň jedno z čísel $a'_{22}, \dots, a'_{r2}$ nenulové, pak toho opět můžeme dosáhnout záměnou řádků. Jsou-li všechna čísla $a'_{22}, \dots, a'_{r2}$ rovna nule, pak můžeme přečíslovat sloupce, ovšem ve výsledku se musíme vrátit k původnímu označení.) Pro každé $j = 3, \dots, r$ přičteme $(-\frac{a'_{j2}}{a'_{22}})$-násobek druhého řádku nové matice k $j$-tému řádku této matice. Opět vynecháme všechny řádky, které obsahují samé nuly. Ve výsledku dostaneme matici, v jejímž 2. sloupci jsou všechny prvky počínaje 3. řádkem rovny nule.

Tímto způsobem pokračujeme tak dlouho, až dojdeme k matici tvaru

$$\left(\begin{array}{ccccc|c} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} & b_1 \\ 0 & a'_{22} & a'_{23} & \cdots & a'_{2n} & b'_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & c_{hh} & \cdots & c_{hn} & d_h \end{array}\right),$$

kde $h \leq n$ a všechny prvky $a_{11}, a'_{22}, \dots, c_{hh}$ na hlavní diagonále jsou nenulové.

Z rovnice

$$c_{hh}\xi_h + \cdots + c_{hn}\xi_n = d_h,$$

která odpovídá poslednímu řádku výsledné matice, vyjádříme neznámou $\xi_h$ pomocí neznámých $\xi_{h+1}, \dots, \xi_n$. Z předposlední rovnice pak analogicky vyjádříme neznámou $\xi_{h-1}$, atd., až z první rovnice vypočítáme neznámou $\xi_1$.

Přitom je zřejmé, že pokud $h = n$, pak má soustava odpovídající poslední matici (a tedy podle věty 7.11 i původní soustava $A, \overrightarrow{\xi}^T = \overrightarrow{b}^T$) jediné řešení, zatímco v případě $h < n$ mají tyto soustavy nekonečně mnoho řešení, která závisejí na $n - h$ parametrech $\xi_{h+1}, \dots, \xi_n$. (Za tyto parametry můžeme dosazovat libovolná čísla z $T$.)

d) Podle Frobeniovy věty platí, že daná soustava není řešitelná, právě když hodnost její rozšíření matice je větší než hodnost její matice. Proto pokud soustava nemá řešení, nutně v průběhu výpočtu pomocí Gaussovy metody dostaneme takovou matici, v níž alespoň jeden její řádek odpovídá rovnici typu $0 = b$, kde $b$ je nenulové číslo.

**Příklad 7.5** Určete množinu řešení soustavy

$$a)\ \begin{aligned} \xi_1+2\xi_2+5\xi_3 &= -9,\\ \xi_1-\xi_2+3\xi_3 &= 2,\\ 3\xi_1-6\xi_2-\xi_3 &= 25. \end{aligned} \qquad b)\ \begin{aligned} 3\xi_1-5\xi_2+2\xi_3+4\xi_4 &= 2,\\ 7\xi_1-4\xi_2+\xi_x3+3\xi_4 &= 5,\\ 5\xi_1+7\xi_2-4\xi_3-6\xi_4 &= 3. \end{aligned}$$

$$c)\ \begin{aligned} 6\xi_1-2\xi_2+2\xi_3+5\xi_4+7\xi_5 &= 0,\\ 9\xi_1-3\xi_2+4\xi_3+8\xi_4+9\xi_5 &= 0,\\ 6\xi_1-2\xi_2+6\xi_3+7\xi_4+\xi_5 &= 0,\\ 3\xi_1-\xi_2+4\xi_3+4\xi_4-\xi_5 &= 0, \end{aligned}.$$

a) Soustavu budeme řešit pomocí Gaussovy metody:

$$\left(\begin{array}{ccc|c} 1 & 2 & 5 & -9\\ 1 & -1 & 3 & 2\\ 3 & -6 & -1 & 25 \end{array}\right) \overset{\check{r}}{\sim} \left(\begin{array}{ccc|c} 1 & 2 & 5 & -9\\ 0 & -3 & -2 & 11\\ 0 & -12 & -16 & 52 \end{array}\right) \overset{\check{r}}{\sim}$$

$$\overset{\check{r}}{\sim} \left(\begin{array}{ccc|c} 1 & 2 & 5 & -9\\ 0 & 3 & 2 & -11\\ 0 & 3 & 4 & -13 \end{array}\right) \overset{\check{r}}{\sim} \left(\begin{array}{ccc|c} 1 & 2 & 5 & -9\\ 0 & 3 & 2 & -11\\ 0 & 0 & 2 & -2 \end{array}\right)$$

Z poslední matice je vidět, že hodnost matice i hodnost její rozšířené matice je rovna 3, tedy soustava je řešitelná, a protože počet řádků v poslední matici je stejný jako počet neznámých (tj. společná hodnost obou matic je rovna počtu neznámých), má tato soustava jediné řešení. Tímto řešením je uspořádaná trojice $(2,-3,-1)$.

b) Analogicky

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

$$\overset{\check{r}}{\sim} \left(\begin{array}{cccc|c} 7 & -4 & 1 & 3 & 5\\ -11 & 3 & 0 & -2 & -8\\ 33 & -9 & 0 & 6 & 23 \end{array}\right) \overset{\check{r}}{\sim} \left(\begin{array}{cccc|c} 7 & -4 & 1 & 3 & 5\\ -11 & 3 & 0 & -2 & -8\\ 0 & 0 & 0 & 0 & -1 \end{array}\right).$$

Vidíme, že hodnost matice poslední soustavy je 2, zatímco hodnost rozšířené matice je 3. Podle Frobeniovy věty proto poslední soustava (a tedy také původní soustava) nemá řešení.

c) Protože se jedná o homogenní soustavu, budeme místo s rozšířenou maticí pracovat s maticí dané soustavy.

$$\begin{pmatrix} 6 & -2 & 2 & 5 & 7\\ 9 & -3 & 4 & 8 & 9\\ 6 & -2 & 6 & 7 & 1\\ 3 & -1 & 4 & 4 & -1 \end{pmatrix} \overset{\check{r}}{\sim} \begin{pmatrix} 3 & -1 & 4 & 4 & -1\\ 6 & -2 & 2 & 5 & 7\\ 9 & -3 & 4 & 8 & 9\\ 6 & -2 & 6 & 7 & 1 \end{pmatrix} \overset{\check{r}}{\sim}$$

$$\begin{pmatrix} 3 & -1 & 4 & 4 & -1 \\ 0 & 0 & -6 & -3 & 9 \\ 0 & 0 & -8 & -4 & 12 \\ 0 & 0 & -2 & -1 & 3 \end{pmatrix} \overset{ř}{\sim} \begin{pmatrix} 3 & -1 & 4 & 4 & -1 \\ 0 & 0 & -2 & -1 & 3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Vynecháme-li poslední dva řádky, (které odpovídají rovnicím ve tvaru $0 = 0$), dostaneme rovnici

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

Protože tato matice má hodnost 2, má soustava nekonečně mnoho řešení závislých na 3 parametrech. Pomocí neznámých $\xi_1, \xi_3, \xi_5$ vyjádříme z 2. rovnice výsledné soustavy neznámou $\xi_4$ a z první rovnice neznámou $\xi_2$. Platí

$$\xi_4 = -2\xi_3 + 3\xi_5, \quad \xi_2 = 3\xi_1 - 4\xi_3 + 11\xi_5.$$

Obecně tedy můžeme zapsat řešení ve tvaru vektoru

$$(\xi_1, 3\xi_1 - 4\xi_3 + 11\xi_5, \xi_3, -2\xi_3 + 3\xi_5, \xi_5).$$

Konkrétní řešení pak dostaneme dosazením za neznámé $\xi_1, \xi_3, \xi_5$. Např. pro $\xi_1 = 2, \xi_3 = -1, \xi_5 = -1$ dostaneme řešení $(2, -1, -1, -1, -1)$, pro $\xi_1 = \xi_3 = \xi_5 = 5$ dostaneme $(0, 0, 0, 0, 0)$.

(Nulový vektor je řešením každé homogenní soustavy, proto takové řešení budeme nazývat *triviální*.)

Nyní se budeme věnovat jiné metodě řešení soustav lineárních rovnic, která má hlavní použití tehdy, když nemusíme znát celé řešení, ale jenom některou jeho složku.

**Věta 7.12 (Cramerovo pravidlo)** *Nechť $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$ je soustava $n$ lineárních rovnic o $n$ neznámých $(n \geq 1)$ nad $\mathcal{T}$ taková, že $\det A \neq 0$. Potom pro každé $j = 1, \ldots, n$ platí*

$$\xi_j = \frac{\det A_j}{\det A},$$

*kde $A_j$ je matice, která vznikne z $A$ nahrazením $j$-tého sloupce vektorem $\overrightarrow{b}^T$.*

D ů k a z: Vynásobíme-li 1. rovnici algebraickým doplňkem $\mathcal{A}_{1j}$ prvku $a_{1j}$, 2. rovnici algebraickým doplňkem $\mathcal{A}_{2j}$ prvku $a_{2j}$, atd. až $n$-tou rovnici algebraickým doplňkem $\mathcal{A}_{nj}$ prvku $a_{nj}$ a získané rovnice sečteme, dostaneme rovnici

$$\underbrace{\sum_{i=1}^{n} \mathcal{A}_{ij} \sum_{k=1}^{n} a_{ik}\xi_k}_{L} = \underbrace{\sum_{i=1}^{n} b_i \mathcal{A}_{ij}}_{\mathrm{P}}.$$

Potom platí

$$L = \sum_{k=1}^{n} \xi_k \sum_{i=1}^{n} a_{ik}\mathcal{A}_{ij},$$

tedy podle Laplaceovy věty dostaneme

$$L = \sum_{k=1}^{n} \xi_k \delta_{jk} \mathrm{det} A = \xi_j \mathrm{det} A.$$

Podle Laplaceovy věty také obdržíme $P = \mathrm{det} A_j$. Celkově proto platí

$$\xi_j \mathrm{det} A = \mathrm{det} A_j,$$

a protože podle předpokladu $\mathrm{det} A \neq 0$, dostáváme rovnost

$$\xi_j = \frac{\mathrm{det} A_j}{\mathrm{det} A}.$$

□

**Příklad 7.6** Vypočítejte neznámou $\xi_4$ ze soustavy

$$\begin{aligned} 2\xi_1 + 3\xi_2 + 11\xi_3 + 5\xi_4 &= 2, \\ \xi_1 + \xi_2 + 5\xi_3 + 2\xi_4 &= 1, \\ 2\xi_1 + \xi_2 + 3\xi_3 + 2\xi_4 &= -3, \\ \xi_1 + \xi_2 + 3\xi_3 + 4\xi_4 &= -3. \end{aligned}$$

Protože determinant matice soustavy je roven 14, můžeme použít Cramerovo pravidlo. Determinant matice $A_4$ (vzniklé nahrazením 4. sloupce původní matice vektorem pravých stran rovnic) je roven -14, proto $\xi_4 = -1$.

Vraťme se nyní k obecnému řešení soustav lineárních rovnic.

**Věta 7.13** *Je-li $A\overrightarrow{\xi}^T = \overrightarrow{o}^T$ homogenní soustava lineárních rovnic o $n$ neznámých nad $\mathcal{T}$ taková, že $h(A) = h$, pak řešení této soustavy tvoří podprostor v aritmetickém vektorovém prostoru $\mathcal{T}^n$. Dimenze tohoto podprostoru je $n - h$.*

D ů k a z:

a) Protože homogenní soustava má vždy alespoň triviální řešení, je množina řešení této soustavy neprázdná. Nechť $\overrightarrow{u}, \overrightarrow{v}$ jsou řešení soustavy, tj. $A\overrightarrow{u}^T = \overrightarrow{o}^T$ a $A\overrightarrow{v}^T = \overrightarrow{o}^T$. Potom platí $A(\overrightarrow{u} + \overrightarrow{v})^T = A(\overrightarrow{u}^T + \overrightarrow{v}^T) = A\overrightarrow{u}^T + A\overrightarrow{v}^T = \overrightarrow{o}^T + \overrightarrow{o}^T = \overrightarrow{o}^T$. Je-li dále $c \in T$, pak $A(c\overrightarrow{u})^T = A(c\overrightarrow{u}^T) = (Ac)\overrightarrow{u}^T = (cA)\overrightarrow{u}^T = c(A\overrightarrow{u}^T) = c\overrightarrow{o}^T = \overrightarrow{o}^T$. Tedy $\overrightarrow{u} + \overrightarrow{v}$ a $c\overrightarrow{u}$ jsou také řešeními dané soustavy, proto podle věty 6.4 tvoří řešení soustavy $A\overrightarrow{\xi}^T = \overrightarrow{o}^T$ podprostor v $\mathcal{T}^n$.

b) Nechť $h(A) = h < n$. Pak existuje $h$ lineárně nezávislých řádků matice $A$ a každý další je jejich lineární kombinací. Můžeme předpokládat pro jednoduchost, že prvních $h$ řádků je lineárně nezávislých a že platí

$$\mathcal{A}_h = \begin{vmatrix} a_{11} & \cdots & a_{1h} \\ \vdots & \ddots & \vdots \\ a_{h1} & \cdots & a_{hh} \end{vmatrix} \neq 0.$$

Protože se zajímáme právě o množinu řešení, můžeme místo soustavy $A\overrightarrow{\xi}^T = \overrightarrow{o}^T$ uvažovat s ní ekvivalentní soustavu skládající se z prvních $h$ rovnic, kterou ještě upravíme na tvar

$$\sum_{k=1}^{h} a_{ik}\xi_k = -\sum_{p=k+1}^{n} a_{ip}\xi_p, \quad i = 1,\dots,h.$$

Matice složená z koeficientů na levých stranách rovnic této soustavy má determinant $\mathcal{A}_h \neq 0$. proto můžeme podle Cramerova pravidla jednoznačně určit obecné řešení, které je závislé na $n-h$ parametrech $\xi_{h+1},\dots,\xi_n$.
Dosaďme za tyto parametry postupně takto:

$$\begin{array}{cccc}
\xi_{h+1} = 1, & \xi_{h+2} = 0, & \dots, & \xi_n = 0, \\
\xi_{h+1} = 0, & \xi_{h+2} = 1, & \dots, & \xi_n = 0, \\
\dots, & \dots, & \dots, & \dots, \\
\xi_{h+1} = 0, & \xi_{h+2} = 0, & \dots, & \xi_n = 1,
\end{array}$$

tedy vždy za právě jeden z parametrů dosazujeme číslo 1 a za ostatní číslo 0.
Uvažujme odpovídající řešení soustavy:

$$\begin{array}{rl}
\overrightarrow{u_1} &= (u_{11}, u_{12}, \dots, u_{1h}, 1, 0, \dots, 0), \\
\overrightarrow{u_2} &= (u_{21}, u_{22}, \dots, u_{2h}, 0, 1, \dots, 0), \\
& \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\
\overrightarrow{u_{n-h}} &= (u_{n-h,1}, u_{n-h,2}, \dots, u_{n-h,h}, 0, 0, \dots, 1).
\end{array}$$

Je zřejmé, že vektory $\overrightarrow{u_1}, \overrightarrow{u_2}, \dots, \overrightarrow{u_{n-h}}$ jsou lineárně nezávislé, a přitom každé další řešení soustavy je jejich lineární kombinací. Tedy podprostor řešení v $\mathcal{T}^n$ dané homogenní soustavy má dimenzi $n-h$.
V případě $h(A) = n$ je počet neznámých v upravované soustavě stejný jako počet zbylých rovnic, proto uvažované obecné řešení nezávisí na parametrech, a existuje tedy jediné (a to triviální) řešení soustavy. Toto triviální řešení tvoří podprostor v $\mathcal{T}^n$ dimenze 0.

□

**Definice 7.15** Fundamentálním systémem řešení *homogenní soustavy lineárních rovnic rozumíme libovolnou bázi prostoru řešení této soustavy.*

`Poznámka:`

a) Protože každá báze prostoru generuje tento prostor, je fundamentálním systémem řešení jednoznačně určena celá množina řešení dané homogenní soustavy lineárních rovnic.

b) Je-li matice soustavy $A\overrightarrow{\xi}^T = \overrightarrow{o}^T$ čtvercová, pak má soustava jen triviální řešení právě tehdy, když $\det A \neq 0$.

**Příklad 7.7** Určete fundamentální systém řešení soustavy

$$\begin{aligned} \xi_1 + 2\xi_2 - \xi_3 + 3\xi_4 - 2\xi_5 &= 0, \\ 2\xi_1 + \xi_2 + \xi_4 - \xi_5 &= 0, \\ 5\xi_1 + 4\xi_2 - \xi_3 + 5\xi_4 - 8\xi_5 &= 0, \\ 3\xi_2 - 2\xi_3 + 5\xi_4 - \xi_5 &= 0. \end{aligned}$$

Nejdříve určíme obecné řešení soustavy:

$$\begin{pmatrix} 1 & 2 & -1 & 3 & -2 \\ 2 & 1 & 0 & 1 & -3 \\ 5 & 4 & -1 & 5 & -8 \\ 0 & 3 & -2 & 5 & -1 \end{pmatrix} \overset{\check{r}}{\sim} \begin{pmatrix} 1 & 2 & -1 & 3 & -2 \\ 2 & 1 & 0 & 1 & -3 \\ 4 & 2 & 0 & 2 & -6 \\ -2 & -1 & 0 & -1 & 3 \end{pmatrix} \overset{\check{r}}{\sim} \begin{pmatrix} 1 & 2 & -1 & 3 & -2 \\ 2 & 1 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Vidíme, že $h(A) = 2$, proto obecné řešení bude obsahovat 3 parametry. Zvolme za parametry neznámé $\xi_1$, $\xi_2$, $\xi_5$. (Samozřejmě to není jediná možná volba. Jinou volbu parametrů dostaneme jiný tvar obecného řešení, které ale určuje stejnou množinu řešení.) Postupně z druhé a první rovnice vypočítáme zbývající neznámé:

$$\begin{aligned} \xi_4 &= -2\xi_1 - \xi_2 + 3\xi_5, \\ \xi_3 &= -5\xi_1 - \xi_2 + 7\xi_5. \end{aligned}$$

Obecné řešení je tedy ve tvaru $(\xi_1, \xi_2, -5\xi_1 - \xi_2 + 7\xi_5, -2\xi_1 - \xi_2 + 3\xi_5, \xi_5)$. Fundamentální systém řešení pak získáme např. podle důkazu věty 7.13 postupnou volbou parametrů

$$\xi_1 = 1, \xi_2 = \xi_5 = 0;$$

$$\xi_1 = 0, \xi_2 = 1, \xi_5 = 0;$$

$$\xi_1 = \xi_2 = 0, \xi_5 = 1.$$

Dostaneme tak vektory $\overrightarrow{u_1} = (1, 0, -5, -2, 0), \overrightarrow{u_2} = (0, 1, -1, -1, 0), \overrightarrow{u_3} = (0, 0, 7, 3, 1)$.

Ukážeme si ještě vztah mezi množinami řešení homogenních a nehomogenních soustav lineárních rovnic.

**Definice 7.16** *Je-li $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$ nehomogenní soustava lineárních rovnic, pak řekneme, že homogenní soustava $A\overrightarrow{\xi}^T = \overrightarrow{o}^T$ je přiřazená soustavě $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$.*

**Věta 7.14** *Nechť $\overrightarrow{u}$ je (pevné) řešení nehomogenní soustavy $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$ lineárních rovnic o $n$ neznámých nad $\mathcal{T}$. Potom množina všech řešení této soustavy je tvořena právě všemi vektory tvaru $\overrightarrow{u} + \overrightarrow{v} \in \mathcal{T}^n$, kde $\overrightarrow{v}$ je libovolné řešení přiřazené homogenní soustavy.*

D ů k a z: Platí-li $A\overrightarrow{v}^T = \overrightarrow{o}^T$, pak $A(\overrightarrow{u} + \overrightarrow{v})^T = A\overrightarrow{u}^T + A\overrightarrow{v}^T = \overrightarrow{b}^T + \overrightarrow{o}^T = \overrightarrow{b}^T$, tedy vektor $\overrightarrow{u} + \overrightarrow{v}$ je řešením soustavy $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$.

Obráceně, nechť $A\overrightarrow{z}^T = \overrightarrow{b}^T$. Pak pro $\overrightarrow{v} = \overrightarrow{z} - \overrightarrow{u}$ platí $A\overrightarrow{v}^T = A(\overrightarrow{z} - \overrightarrow{u})^T = A\overrightarrow{z}^T - A\overrightarrow{u}^T = \overrightarrow{b}^T - \overrightarrow{b}^T = \overrightarrow{o}^T$, tedy $\overrightarrow{v}$ je řešením soustavy $A\overrightarrow{\xi}^T = \overrightarrow{o}^T$, a přitom $\overrightarrow{z} = \overrightarrow{u} + \overrightarrow{v}$. □

**Věta 7.15** *Nechť* $A \in M_n(\mathcal{T})$, $\overrightarrow{b} \in \mathcal{T}^n$. *Pak soustava* $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$ *má jediné řešení, právě když* $\det A \neq 0$. *Soustava* $A\overrightarrow{\xi}^T = \overrightarrow{b}^T$ *má nekonečně mnoho řešení nebo nemá žádné řešení právě tehdy, když* $\det A = 0$.

D ů k a z: Tvrzení je přímým důsledkem věty 7.14 a poznámky b) za definicí 7.15. □

## 7.4 Cvičení

**7.1** Vypočítejte hodnost matice

$$a)\begin{pmatrix} 5 & -3 & 2 & 3 & 4 \\ 2 & 1 & 4 & -3 & 7 \\ 11 & -4 & -7 & 4 & -7 \\ 7 & 5 & 1 & -11 & 6 \end{pmatrix};\, b)\begin{pmatrix} 2 & -2 & 1 & 8 & 2 \\ 5 & -3 & 5 & 1 & 6 \\ -1 & 1 & 3 & 2 & -3 \end{pmatrix}.$$

[ a) 3; b) 3 ]

**7.2** Určete hodnoty $\lambda$, pro které má matice

$$\begin{pmatrix} 3 & 1 & 1 & 4 \\ \lambda & 4 & 10 & 1 \\ 1 & 7 & 17 & 3 \\ 2 & 2 & 4 & 3 \end{pmatrix}$$

nejmenší hodnost.
[ $\lambda = 0$ ]

**7.3** Vypočítejte hodnost matice

$$\begin{pmatrix} 1 & \lambda & -1 & 2 \\ 2 & -1 & \lambda & 5 \\ 1 & 10 & -6 & 1 \end{pmatrix}$$

v závislosti na parametru $\lambda$.
[ Pro $\lambda = 3$ je hodnost rovna 2, pro ostatní hodnoty $\lambda$ je hodnost rovna 3. ]

**7.4** Rozhodněte, je-li řešitelná následující soustava lineárních rovnic. V kladném případě určete obecné řešení.

$$a)\begin{aligned} 2\xi_1 - 3\xi_2 + 5\xi_3 + 7\xi_4 &= 1, \\ 4\xi_1 - 6\xi_2 + 2\xi_3 + 3\xi_4 &= 2, \\ 2\xi_1 - 3\xi_2 - 11\xi_3 - 15\xi_4 &= 1; \end{aligned} \qquad b)\begin{aligned} 2\xi_1 + 5\xi_2 - 8\xi_3 &= 8, \\ 4\xi_1 + 3\xi_2 - 9\xi_3 &= 9, \\ 2\xi_1 + 3\xi_2 - 5\xi_3 &= 7, \\ \xi_1 + 8\xi_2 - 7\xi_3 &= 12; \end{aligned}$$

$$c)\quad \begin{aligned} 2\xi_1 - \xi_2 + 3\xi_3 - 2\xi_4 &= 4, \\ 8\xi_1 + 5\xi_2 + 9\xi_3 &= -2, \\ 5\xi_1 + 2\xi_2 + 6\xi_3 - \xi_4 &= -3. \end{aligned}$$

[ a) řešitelná, obecné řešení např. $(3\xi_2 - \xi_4 + \frac{1}{2}, 2\xi_2, -22\xi_4, 16\xi_4)$; b) řešitelná, jediné řešení $(3, 2, 1)$; c) není řešitelná ]

**7.5** Následující systémy rovnic řešte Gaussovou eliminační metodou:

$$a)\begin{aligned} \xi_1 + 2\xi_2 + \xi_3 + \xi_4 &= 3, \\ \xi_1 + 4\xi_2 + 5\xi_3 + 2\xi_4 &= 2, \\ 2\xi_1 + 9\xi_2 + 8\xi_3 + 3\xi_4 &= 7, \\ 3\xi_1 + 7\xi_2 + 7\xi_3 + 2\xi_4 &= 12, \\ 5\xi_1 + 7\xi_2 + 9\xi_3 + 2\xi_4 &= 20. \end{aligned} \qquad b)\begin{aligned} 10\xi_1 + 23\xi_2 + 17\xi_3 + 44\xi_4 &= 25, \\ 15\xi_1 + 35\xi_2 + 26\xi_3 + 69\xi_4 &= 40, \\ 25\xi_1 + 57\xi_2 + 42\xi_3 + 108\xi_4 &= 65, \\ 30\xi_1 + 69\xi_2 + 51\xi_3 + 133\xi_4 &= 95. \end{aligned}$$

[ a)$\xi_1 = \frac{1}{4}\xi_4 + \frac{31}{6}, \xi_2 = \frac{2}{3}; \xi_3 = -\frac{1}{2}\xi_4 - \frac{7}{6}$; b) nemá řešení ]

**7.6** Najděte obecné řešení a fundamentální systém řešení homogenních soustav:

$$a)\begin{aligned} 3\xi_1 + 2\xi_2 + \xi_3 + 3\xi_4 + 5\xi_5 &= 0, \\ 6\xi_1 + 4\xi_2 + 3\xi_3 + 5\xi_4 + 7\xi_5 &= 0, \\ 9\xi_1 + 6\xi_2 + 5\xi_3 + 7\xi_4 + 9\xi_5 &= 0, \\ 3\xi_1 + 2\xi_2 + 4\xi_4 + 8\xi_5 &= 0. \end{aligned} \qquad b)\begin{aligned} \xi_1 - \xi_3 &= 0, \\ \xi_2 - \xi_4 &= 0, \\ -\xi_1 + \xi_3 - \xi_5 &= 0, \\ -\xi_2 + \xi_4 - \xi_6 &= 0, \\ -\xi_3 + \xi_5 &= 0, \\ -\xi_4 + \xi_6 &= 0. \end{aligned}$$

[ a) $\xi_4 = -\frac{9\xi_1+6\xi_2+8\xi_3}{4}$, $\xi_5 = \frac{3\xi_1+2\xi_2+4\xi_3}{4}$; $(1, 0, 0, -\frac{9}{4}, \frac{3}{4})$, $(0, 1, 0, -\frac{3}{2}, \frac{1}{2})$, $(0, 0, 1, -2, 1)$; b) pouze jediné (nulové) řešení ]

**7.7** Určete množinu řešení soustavy

$$\begin{aligned} \lambda\xi_1 + \xi_2 + \xi_3 + \xi_4 &= 1, \\ \xi_1 + \lambda\xi_2 + \xi_3 + \xi_4 &= 1, \\ \xi_1 + \xi_2 + \lambda\xi_3 + \xi_4 &= 1, \\ \xi_1 + \xi_2 + \xi_3 + \lambda\xi_4 &= 1. \end{aligned}$$

v závislosti na parametru $\lambda$.

[ Jestliže $\lambda \neq 1$ a $\lambda \neq -3$, pak má soustava jediné řešení $(\frac{1}{\lambda+3}, \frac{1}{\lambda+3}, \frac{1}{\lambda+3}, \frac{1}{\lambda+3})$. Pro $\lambda = 1$, má soustava obecné řešení $(1 - \xi_2 - \xi_3 - \xi_4, \xi_2, \xi_3, \xi_4)$. Pro $\lambda = -3$ není soustava řešitelná. ]

**7.8** Najděte obecné řešení v závislosti na parametru $\lambda$.

$$a)\begin{aligned} 5\xi_1 - 3\xi_2 + 2\xi_3 + 4\xi_4 &= 3, \\ 4\xi_1 - 2\xi_2 + 3\xi_3 + 7\xi_4 &= 1, \\ 8\xi_1 - 6\xi_2 - \xi_3 - 5\xi_4 &= 9, \\ 7\xi_1 - 3\xi_2 + 7\xi_3 + 17\xi_4 &= \lambda. \end{aligned} \qquad b)\begin{aligned} 2\xi_1 + 5\xi_2 + \xi_3 + 3\xi_4 &= 2, \\ 4\xi_1 + 6\xi_2 + 3\xi_3 + 5\xi_4 &= 4, \\ 4\xi_1 + 14\xi_2 + \xi_3 + 7\xi_4 &= 4, \\ 2\xi_1 - 3\xi_2 + 3\xi_3 + \lambda\xi_4 &= 7. \end{aligned}$$

[ a)$\lambda \neq 0$ nemá řešení, $\lambda = 0$ $\xi_1 = \frac{-5\xi_3-13\xi_4-3}{2}$, $\xi_2 = \frac{-7\xi_3-19\xi_4-7}{2}$; b) $\lambda = 1$ nemá řešení, $\lambda \neq 1$ $\xi_1 = \frac{43-8\lambda}{8-8\lambda} - \frac{9}{8}\xi_3$, $\xi_2 = \frac{5}{4-4\lambda} + \frac{1}{4}\xi_3$, $\xi_4 = \frac{5}{\lambda-1}$ ]

**7.9** Zjistěte, tvoří-li řádky matice

$$A = \begin{pmatrix} 4 & 2 & 9 & -20 & -3 \\ 1 & -11 & 2 & 13 & 4 \\ 9 & -15 & 8 & 5 & 2 \end{pmatrix}$$

fundamentální systém řešení soustavy rovnic

$$\begin{aligned} 3\xi_1 + 4\xi_2 + 2\xi_3 + \xi_4 + 6\xi_5 &= 0, \\ 5\xi_1 + 9\xi_2 + 7\xi_3 + 4\xi_4 + 7\xi_5 &= 0, \\ 4\xi_1 + 3\xi_2 - \xi_3 - \xi_4 + 11\xi_5 &= 0, \\ \xi_1 + 6\xi_2 + 8\xi_3 + 5\xi_4 - 4\xi_5 &= 0. \end{aligned}$$

[ tvoří ]

**7.10** Vypočítejte pomocí Cramerova pravidla neznámou $\xi_2$ ze soustavy

$$\begin{aligned} 2\xi_1 + 5\xi_2 + 4\xi_3 + \xi_4 &= 20, \\ \xi_1 + 3\xi_2 + 2\xi_3 + \xi_4 &= 11, \\ 2\xi_1 + 10\xi_2 + 9\xi_3 + 7\xi_4 &= 40, \\ 3\xi_1 + 8\xi_2 + 9\xi_3 + 2\xi_4 &= 37. \end{aligned}$$

[ $\xi_2 = 2$ ]

**7.11** Následující systémy rovnic řešte Cramerovým pravidlem:

$$a)\begin{aligned} 2\xi_1 + 2\xi_2 - \xi_3 + \xi_4 &= 4, \\ 4\xi_1 + 3\xi_2 - \xi_3 + 2\xi_4 &= 6, \\ 8\xi_1 + 5\xi_2 - 3\xi_3 + 4\xi_4 &= 12, \\ 3\xi_1 + 3\xi_2 - 2\xi_3 + 2\xi_4 &= 6. \end{aligned} \qquad b)\begin{aligned} 2\xi_1 + 5\xi_2 + 4\xi_3 + \xi_4 &= 20, \\ \xi_1 + 3\xi_2 + 2\xi_3 + \xi_4 &= 11, \\ 2\xi_1 + 10\xi_2 + 9\xi_3 + 7\xi_4 &= 40, \\ 3\xi_1 + 8\xi_2 + 9\xi_3 + 2\xi_4 &= 37. \end{aligned}$$

[ a)$\xi_1 = \xi_2 = 1, \xi_3 = \xi_4 = -1$; b)$\xi_1 = 1, \xi_2 = \xi_3 = 2, \xi_4 = 0$ ]

# Kapitola 8

# Okruh čtvercových matic

Na základě věty 4.6 víme že množina $M_n(\mathcal{T})$ všech čtvercových matic stupně $n$ nad $\mathcal{T}$ spolu se sčítáním a násobením matic tvoří okruh $\mathcal{M}_n(\mathcal{T})$, který pro $n > 1$ není komutativní a obsahuje netriviální dělitele nuly. V této části si všimneme blíže vlastností tohoto okruhu.

## 8.1 Regulární a singulární matice

**Definice 8.1**

*a) Matice* $A \in M_n(\mathcal{T})$ *se nazývá* regulární, *platí-li* $\det A \neq 0$.

*b) Matice* $A \in M_n(\mathcal{T})$ *se nazývá* singulární, *platí-li* $\det A = 0$.

**Věta 8.1** *Regulární matice z* $M_n(\mathcal{T})$ *tvoří multiplikativní pologrupu s jednotkovým prvkem.*

(Později dokážeme, že tato pologrupa je dokonce grupou.)

D ů k a z: Nechť $A, B \in M_n(\mathcal{T})$, $\det A \neq 0 \neq \det B$. Potom podle věty 5.23 platí

$$\det AB = \det A \cdot \det B \neq 0,$$

tedy $AB$ je regulární.

Obecně platí, že násobení matic je asociativní, proto $(M_n(\mathcal{T}), \cdot)$ je pologrupa. Přitom jednotkovým prvkem v této pologrupě je jednotková matice $E_n$. □

**Věta 8.2** *Jsou-li* $A, B \in M_n(\mathcal{T})$ *a platí-li, že* $\det AB = 0$, *pak* $\det A = 0$ *nebo* $\det B = 0$.

D ů k a z: Tvrzení plyne z věty 8.1. □

**Věta 8.3** *V okruhu* $\mathcal{M}_n(\mathcal{T}) = (M_n(\mathcal{T}), +, \cdot)$ *jsou děliteli nuly právě všechny singulární matice.*

D ů k a z: Nulová matice $N$ (která má determinant roven 0) je vždy levým i pravým dělitelem nuly. Proto si v důkazu budeme všímat pouze netriviálních dělitelů nuly.

a) Nechť $N \neq A \in M_n(\mathcal{T})$ je levý netriviální dělitel nuly. Pak existuje $N \neq B \in M_n(\mathcal{T})$ tak, že $AB = N$. V matici $B = ||\overrightarrow{b_1}', \dots, \overrightarrow{b_n}'||$ potom existuje alespoň jeden nenulový sloupec $\overrightarrow{b_j}'$. Platí tedy $A\overrightarrow{b_j}' = \overrightarrow{o}'$, a proto je $\overrightarrow{b_j}$ netriviálním řešením soustavy $A\overrightarrow{\xi}' = \overrightarrow{o}'$. To ovšem znamená (podle poznámky za definicí 7.15, že $\det A = 0$, tj. $A$ je singulární.

b) Nechť $A \in M_n(\mathcal{T})$ a nechť $\det A = 0$. Pak má soustava $A\overrightarrow{\xi}' = \overrightarrow{o}'$alespoň jedno netriviální řešení, např. $\overrightarrow{b_1}$. Uvažujme potom matici $B = ||\overrightarrow{b_1}', \overrightarrow{o}', \dots, \overrightarrow{o}'||$, která je různá od $N$. Protože platí $AB = N$, je $A$ levým netriviálním dělitelem nuly.

c) Nechť $A \in M_n(\mathcal{T})$ je levý netriviální dělitel nuly. Pak $\det A^T = \det A = 0$, takže $A^T$ je podle části b) také levý netriviální dělitel nuly. Proto v okruhu $\mathcal{M}_n(\mathcal{T})$ existuje matice $D^T \neq N$ taková, že $A^T D^T = N$, tedy $DA = N^T = N$. Proto je $A$ také pravý netriviální dělitel nuly.

□

**Definice 8.2** *Jestliže k matici $A \in M_n(\mathcal{T})$ existuje inverzní prvek $A^{-1}$ v pologrupě $(M_n(\mathcal{T}), \cdot)$, pak se matice $A^{-1}$ nazývá* inverzní matice k matici *$A$.*

**Věta 8.4** *Je-li $A$ matice z $M_n(\mathcal{T})$, potom k ní existuje inverzní matice $A^{-1}$ tehdy a jen tehdy, je-li matice $A$ regulární.*

D ů k a z:

a) Nechť $\det A = 0$. Existuje-li matice $B \in M_n(\mathcal{T})$ taková, že $AB = E$ (inverzní matice $A^{-1}$ k matici $A$ musí splňovat $AA^{-1} = E = A^{-1}A$), potom podle věty 5.23 platí $\det A \cdot \det B = \det E$, tj. $0 \cdot \det B = 1$, což je spor. Proto taková matice $B$ nemůže existovat, a tedy nemůže existovat ani matice $A^{-1}$.

b) Nechť $A = ||a_{ik}|| \in M_n(\mathcal{T})$, $\det A \neq 0$. Označme $\mathrm{adj} A = ||\mathcal{A}_{ki}||$, kterou nazveme *matice adjungovaná k matici* $A$. (Matice $\mathrm{adj}A$ je tedy transponovaná matice k matici sestavené z algebraických doplňků prvků matice $A$.) Podle Laplaceovy věty nyní platí

$$A \cdot \mathrm{adj}A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} \mathcal{A}_{11} & \mathcal{A}_{21} & \cdots & \mathcal{A}_{n1} \\ \mathcal{A}_{12} & \mathcal{A}_{22} & \cdots & \mathcal{A}_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{A}_{1n} & \mathcal{A}_{2n} & \cdots & \mathcal{A}_{nn} \end{pmatrix} =$$

$$= \begin{pmatrix} \det A & a_{12} & \cdots & 0 \\ 0 & \det A & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \det A \end{pmatrix} = \mathrm{adj}A \cdot A.$$

Proto platí také
$$A \cdot (\frac{1}{\mathrm{det} A}\mathrm{adj} A) = E = (\frac{1}{\mathrm{det} A}\mathrm{adj} A) \cdot A.$$
To ovšem znamená, že matice $A^{-1}$ existuje a že platí
$$A^{-1} = \frac{1}{\mathrm{det} A}\mathrm{adj} A.$$
□

**Věta 8.5** *Regulární matice stupně $n$-tého tvoří multiplikativní grupu.*

D ů k a z: Podle věty 8.1 víme, že množina všech regulárních matic stupně $n$ je multiplikativní pologrupou s jednotkovým prvkem. Zbývá tedy dokázat, že inverzní matice k regulární matici $A$ (která existuje podle věty 8.4) je také regulární.

Ovšem kdyby platilo, že matice $A^{-1}$ je singulární (tj. $\mathrm{det} A^{-1} = 0$), pak by platilo (protože $\mathrm{det} A \cdot \mathrm{det} A^{-1} = \mathrm{det} E$), že $\mathrm{det} A \cdot 0 = 1$, což je spor. To ovšem znamená, že matice $A^{-1}$ je také regulární, a proto je inverzním prvkem k matici $A$ v pologrupě $(M_n(\mathcal{T}), \cdot)$. □

**Věta 8.6** *Jsou-li $A, B$ regulární matice z $M_n(\mathcal{T})$, pak platí*
$$(AB)^{-1} = B^{-1}A^{-1}.$$

D ů k a z: Platí $(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AEA^{-1} = AA^{-1} = E$ a podobně $(B^{-1}A^{-1})(AB) = E$. □

**Příklad 8.1** Určeme inverzní matici k matici
$$A = \begin{pmatrix} 2 & -1 & 3 \\ 1 & -1 & -2 \\ -3 & 2 & 1 \end{pmatrix}.$$

Protože det $= -2$, je $A$ regulární, a proto inverzní matice $A^{-1}$ existuje. Určíme nejdříve matici adj$A$.

$$\mathcal{A}_{11} = \begin{vmatrix} -1 & -2 \\ 2 & 1 \end{vmatrix} = 3, \quad \mathcal{A}_{12} = -\begin{vmatrix} 1 & -2 \\ -3 & 1 \end{vmatrix} = 5, \quad \mathcal{A}_{13} = \begin{vmatrix} 1 & -1 \\ -3 & 2 \end{vmatrix} = -1,$$
$$\mathcal{A}_{21} = -\begin{vmatrix} -1 & 3 \\ 2 & 1 \end{vmatrix} = 7, \quad \mathcal{A}_{22} = \begin{vmatrix} 2 & 3 \\ -3 & 1 \end{vmatrix} = 11, \quad \mathcal{A}_{23} = -\begin{vmatrix} 2 & -1 \\ -3 & 2 \end{vmatrix} = -1,$$
$$\mathcal{A}_{31} = \begin{vmatrix} -1 & 3 \\ -1 & -2 \end{vmatrix} = 5, \quad \mathcal{A}_{32} = -\begin{vmatrix} 2 & 3 \\ 1 & -2 \end{vmatrix} = 7, \quad \mathcal{A}_{33} = \begin{vmatrix} 2 & -1 \\ 1 & -1 \end{vmatrix} = -1,$$

$$\mathrm{adj}A = \begin{pmatrix} 3 & 7 & 5 \\ 5 & 11 & 7 \\ -1 & -1 & -1 \end{pmatrix}.$$

Nyní už vypočítáme inverzní matici.

$$\mathrm{adj}A^{-1} = -\frac{1}{2}\mathrm{adj}A = \begin{pmatrix} -\frac{3}{2} & -\frac{7}{2} & -\frac{5}{2} \\ -\frac{5}{2} & -\frac{11}{2} & -\frac{7}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

## 8.2 Výpočet inverzní matice pomocí elementárních transformací

Nyní si ukážeme jiný způsob výpočtu inverzní matice k dané regulární matici, který si nevyžaduje výpočet adjungované matice.

**Definice 8.3** *Nechť je dána libovolná elementární řádková transformace čtvercové matice $n$-tého stupně. Potom* maticí této elementární transformace *rozumíme matici, která vznikne z jednotkové matice $n$-tého stupně použitím této transformace.*

**Věta 8.7** *Je-li $A \in M_n(\mathcal{T})$, pak jsou si rovny matice, které dostaneme z matice $A$*

*a) provedením dané elementární řádkové transformace na $A$;*

*b) vynásobením matice $A$ maticí této transformace zleva.*

D ů k a z: Nechť $A = ||a_{ij}|| \in M_n(\mathcal{T})$.

a) Předpokládejme, že jsme zaměnili první a druhý řádek, a vynásobme matici $A$ maticí této transformace zleva. Dostaneme

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} = \begin{pmatrix} a_{21} & a_{22} & \cdots & a_{2n} \\ a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

b) Předpokládejme, že jsme vynásobili první řádek prvkem $c \in T$, $c \neq 0$. Přitom po vynásobení matice $A$ příslušnou maticí elementární řádkové transformace zleva dostaneme

$$\begin{pmatrix} c & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} = \begin{pmatrix} ca_{11} & ca_{12} & \cdots & ca_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

c) Konečně předpokládejme, že jsme ke druhému řádku přičetli $c$-násobek prvního řádku. Po vynásobení maticí příslušné elementární transformace zleva dostaneme

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ c & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ ca_{11}+a_{21} & ca_{12}+a_{22} & \cdots & ca_{1n}+a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

(Přitom omezení v bodech a), b), c) nejsou vůbec na úkor obecnosti.) □

**Věta 8.8** *Je-li $A \in M_n(\mathcal{T})$ regulární, pak je možno přejít pomocí elementárních řádkových transformací od matice $A$ k matici $E$. Přitom pomocí stejných transformací přejdeme od matice $E$ k matici $A^{-1}$.*

D ů k a z: Je zřejmé (podle věty 7.7), že pro každou regulární matici $A$ $n$-tého stupně platí $h(A) = n$. Proto podle vět 7.1 a 7.3 je regulární matice řádkově ekvivalentní s jednotkovou maticí, a tedy je možno přejít pomocí elementárních řádkových transformací od matice $A$ k matici $E$. Nechť $B_1 \ldots, B_r$ jsou matice použitých elementárních řádkových transformací, tj. platí

$$E = B_r \ldots B_1 A.$$

Potom

$$EA^{-1} = B_r \ldots B_1 AA^{-1},$$

tedy

$$A^{-1} = B_r \ldots B_1 E,$$

proto $A^{-1}$ dostaneme z matice $E$ pomocí elementárních řádkových transformací odpovídajících maticím $B_1, \ldots, B_r$. □

**Příklad 8.2** Vypočítejme pomocí elementárních řádkových transformací inverzní matici $A^{-1}$ ke stejné matici

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

jako v příkladě 8.1. Jednotlivé elementární řádkové transformace budeme v obou případech provádět současně, což schematicky zapíšeme použitím matic typu $n \times 2n$. Platí tedy

$$\left(\begin{array}{rrr|rrr} 2 & -1 & 3 & 1 & 0 & 0 \\ 1 & -1 & -2 & 0 & 1 & 0 \\ -3 & 2 & 1 & 0 & 0 & 1 \end{array}\right) \overset{ř}{\sim} \left(\begin{array}{rrr|rrr} 1 & -1 & -2 & 0 & 1 & 0 \\ 0 & 1 & 7 & 1 & -2 & 0 \\ 0 & -1 & -5 & 0 & 3 & 1 \end{array}\right) \overset{ř}{\sim}$$

$$\overset{ř}{\sim} \left(\begin{array}{rrr|rrr} 1 & -1 & -2 & 0 & 1 & 0 \\ 0 & 1 & 7 & 1 & -2 & 0 \\ 0 & 0 & -1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{array}\right) \overset{ř}{\sim} \left(\begin{array}{rrr|rrr} 1 & -1 & -2 & 0 & 1 & 0 \\ 0 & 1 & 0 & -\frac{5}{2} & -\frac{11}{2} & -\frac{7}{2} \\ 0 & 0 & 1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{array}\right) \overset{ř}{\sim}$$

$$\overset{\check{r}}{\sim}\left(\begin{array}{ccc|ccc} 1 & 0 & -2 & -\frac{5}{2} & -\frac{9}{2} & -\frac{7}{2} \\ 0 & 1 & 0 & -\frac{5}{2} & -\frac{11}{2} & -\frac{7}{2} \\ 0 & 0 & 1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{array}\right) \overset{\check{r}}{\sim}\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{3}{2} & -\frac{7}{2} & -\frac{5}{2} \\ 0 & 1 & 0 & -\frac{5}{2} & -\frac{11}{2} & -\frac{7}{2} \\ 0 & 0 & 1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{array}\right)$$

proto

$$A^{-1} = \begin{pmatrix} -\frac{3}{2} & -\frac{7}{2} & -\frac{5}{2} \\ -\frac{5}{2} & -\frac{11}{2} & -\frac{7}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

## 8.3 Cvičení

**8.1** Určete všechny čtvercové matice $B \neq N$, pro které platí $AB = N$, jestliže

$$a) A = \begin{pmatrix} 3 & 6 \\ -4 & -8 \end{pmatrix}; \qquad b) B = \begin{pmatrix} 5 & 2 & -1 \\ 3 & 1 & 4 \\ -2 & 2 & -3 \end{pmatrix}.$$

[ $a) \begin{pmatrix} -2a & -2b \\ a & b \end{pmatrix}$; b) neexistuje ]

**8.2** Určete inverzní matici k matici

$$a) A = \begin{pmatrix} -5 & -4 \\ 6 & 5 \end{pmatrix}; \qquad b) B = \begin{pmatrix} -1 & 3 & 6 \\ 4 & -2 & 1 \\ 7 & -1 & 7 \end{pmatrix}.$$

[ $a) \begin{pmatrix} -5 & -4 \\ 6 & 5 \end{pmatrix}$; $b) \begin{pmatrix} -\frac{13}{10} & -\frac{27}{10} & \frac{15}{10} \\ -\frac{21}{10} & -\frac{49}{10} & -\frac{25}{10} \\ 1 & 2 & -1 \end{pmatrix}$. ]

**8.3** Vypočítejte matici $X$ z rovnice

a) $\begin{pmatrix} 6 & -5 \\ 4 & -3 \end{pmatrix} X = \begin{pmatrix} -1 & 3 \\ 7 & 2 \end{pmatrix}$;

b) $\begin{pmatrix} 3 & 4 \\ 5 & 7 \end{pmatrix} X \begin{pmatrix} -2 & 5 \\ -4 & 9 \end{pmatrix} = \begin{pmatrix} 3 & 6 \\ -2 & 1 \end{pmatrix}$;

c) $X \begin{pmatrix} 1 & 0 & 1 \\ -2 & 1 & 3 \\ 2 & -1 & 0 \end{pmatrix} = \begin{pmatrix} 6 & -2 & 11 \\ 1 & -1 & - \\ 11 & -4 & 9 \end{pmatrix}$.

[ a) $\begin{pmatrix} 19 & \frac{1}{2} \\ 23 & 0 \end{pmatrix}$; b) $\begin{pmatrix} \frac{413}{2} & -\frac{221}{2} \\ -\frac{297}{2} & \frac{159}{2} \end{pmatrix}$; c) $\begin{pmatrix} 2 & 3 & 5 \\ -1 & 0 & 1 \\ 3 & 2 & 6 \end{pmatrix}$ ]

# Kapitola 9

# Homomorfizmy a izomorfizmy vektorových prostorů

## 9.1 Základní vlastnosti

**Definice 9.1** *Nechť $\mathcal{V} = (V, +, \mathcal{T}, \cdot)$ a $\mathcal{V}' = (V', +, \mathcal{T}, \cdot)$ jsou vektorové prostory nad číselným tělesem $\mathcal{T}$. Potom zobrazení $f : V \to V'$ nazveme* homomorfizmus *vektorového prostoru $\mathcal{V}$ do vektorového prostoru $\mathcal{V}'$, jestliže*

1. $\forall \overrightarrow{u}, \overrightarrow{v} \in V;\ f(\overrightarrow{u} + \overrightarrow{v}) = f(\overrightarrow{u}) + f(\overrightarrow{v})$,
2. $\forall c \in T, \overrightarrow{u} \in V;\ f(c\overrightarrow{u}) = cf(\overrightarrow{u})$.

**Definice 9.2**

a) *Bijektivní homomorfizmus $\mathcal{V}$ na $\mathcal{V}'$ se nazývá* izomorfizmus *$\mathcal{V}$ na $\mathcal{V}'$.*

b) *Řekneme, že vektorový prostor $\mathcal{V}'$ je* izomorfní *s vektorovým prostorem $\mathcal{V}$, existuje-li alespoň jeden izomorfizmus $\mathcal{V}$ na $\mathcal{V}'$.*

**Definice 9.3** *Je-li $f$ homomorfizmus vektorového prostoru $\mathcal{V}$ do vektorového prostoru $\mathcal{V}'$, pak* jádrem homomorfizmu *$f$ nazýváme množinu* $\mathrm{Ker} f = \{\overrightarrow{u} \in V; f(\overrightarrow{u}) = \overrightarrow{o}'\}$. *(Symbol $\overrightarrow{o}'$ označuje nulový vektor ve $\mathcal{V}'$.)*

*Obrazem homomorfizmu $f$* rozumíme množinu $Imf = \{f(\overrightarrow{u}); \overrightarrow{u} \in V\}$.

**Věta 9.1** *Je-li $f$ homomorfizmus $\mathcal{V}$ do $\mathcal{V}'$, pak*

a) *$f$ je injektivní, právě když* $\mathrm{Ker} f = \{\overrightarrow{o}\}$;

b) *$f$ je surjektivní, právě když* $\mathrm{Im} f = \mathcal{V}'$;

c) *$f$ je izomorfizmus, právě když* $\mathrm{Ker} f = \{\overrightarrow{o}\}$ *a* $\mathrm{Im} f = \mathcal{V}'$.

D ů k a z: Stačí dokázat část a), ostatní části jsou pak zřejmé.

a) Je-li $\overrightarrow{u} \in V$, pak $\overrightarrow{o} = 0 \cdot \overrightarrow{u}$, tedy $f(\overrightarrow{o}) = f(0 \cdot \overrightarrow{u}) = 0 \cdot f(\overrightarrow{u}) = \overrightarrow{o}'$, proto vždy $\overrightarrow{o} \in \mathrm{Ker} f$. Je-li $f$ injektivní, pak každý prvek z $\mathcal{V}'$ má nejvýše jeden vzor v homomorfizmu $f$, tedy $\mathrm{Ker} f = \{\overrightarrow{o}\}$.
Obráceně, nechť $\mathrm{Ker} f = \{\overrightarrow{o}\}$ a nechť existují $\overrightarrow{u}, \overrightarrow{v} \in V$, $\overrightarrow{u} \neq \overrightarrow{v}$, takové, že $f(\overrightarrow{u}) = f(\overrightarrow{v})$. Potom $\overrightarrow{o}' = f(\overrightarrow{u}) - f(\overrightarrow{v}) = f(\overrightarrow{u} - \overrightarrow{v})$, což znamená, že $\overrightarrow{u} - \overrightarrow{v} \in \mathrm{Ker} f$. Ovšem $\overrightarrow{u} - \overrightarrow{v} \neq \overrightarrow{o}$, to je spor.

□

**Věta 9.2** *Nechť $\mathcal{V}$, $\mathcal{V}'$, $\mathcal{V}''$ jsou vektorové prostory nad $\mathcal{T}$, $f$ homomorfizmus $\mathcal{V}$ do $\mathcal{V}'$, $g$ homomorfizmus $\mathcal{V}'$ do $\mathcal{V}''$. Potom složené zobrazení $f \circ g : V \to V''$ (tj. $\forall \overrightarrow{u} \in V; (f \circ g)(\overrightarrow{u}) = g(f(\overrightarrow{u}))$) je homomorfizmus $\mathcal{V}$ do $\mathcal{V}''$.*

D ů k a z: Máme ověřit, že zobrazení $f \circ g$ splňuje podmínky 1 a 2 z definice 9.1.

1. Jsou-li $\overrightarrow{u}, \overrightarrow{v} \in V$, pak

$$(f \circ g)(\overrightarrow{u} + \overrightarrow{v}) = g(f(\overrightarrow{u} + \overrightarrow{v})) = g(f(\overrightarrow{u}) + f(\overrightarrow{v})) =$$

$$= g(f(\overrightarrow{u})) + g(f(\overrightarrow{v})) = (f \circ g)(\overrightarrow{u}) + (f \circ g)(\overrightarrow{v}).$$

2. Nechť $c \in T$, $\overrightarrow{u} \in V$. Pak

$$(f \circ g)(c\overrightarrow{u}) = g(f(c\overrightarrow{u})) = g(c(f(\overrightarrow{u}))) = c(g(f(\overrightarrow{u}))) = c[(f \circ g)(\overrightarrow{u})].$$

□

**Věta 9.3** *Je-li $f$ izomorfizmus $\mathcal{V}$ na $\mathcal{V}'$ pak zobrazení $f^{-1} : V' \to V$ je izomorfizmem $\mathcal{V}'$ na $\mathcal{V}$.*

D ů k a z: Pro každý $\overrightarrow{u} \in V$ budeme symbolem $\overrightarrow{u}'$ označovat vektor $f(u) \in V'$ (pro který platí také $f^{-1}(\overrightarrow{u}') = \overrightarrow{u}$).

Nechť $\overrightarrow{u}', \overrightarrow{v}' \in V'$. Pak $f^{-1}(\overrightarrow{u}' + \overrightarrow{v}') = f^{-1}(f(\overrightarrow{u}) + f(\overrightarrow{v})) = f^{-1}(f(\overrightarrow{u} + \overrightarrow{v})) = \overrightarrow{u} + \overrightarrow{v} = f^{-1}(\overrightarrow{u}') + f^{-1}(\overrightarrow{v}')$.

Dále předpokládejme, že $c \in T$, $\overrightarrow{u}' \in V'$. Pak $f^{-1}(c\overrightarrow{u}') = f^{-1}(cf(\overrightarrow{u})) = f^{-1}(f(c\overrightarrow{u})) = c\overrightarrow{u} = cf^{-1}(\overrightarrow{u}')$.

Tím jsme ověřili, že $f^{-1}$ je homomorfizmus, a protože je bijektivní, je také izomorfizmem. □

`Poznámka`: Ověřili jsme tak, že vektorový prostor $\mathcal{V}'$ je izomorfní s vektorovým prostorem $\mathcal{V}$, právě když $\mathcal{V}$ je izomorfní s $\mathcal{V}'$. V takovém případě budeme také říkat, že $\mathcal{V}$ a $\mathcal{V}'$ *jsou izomorfní*. V dalším uvidíme, že z algebraického hlediska nemusíme rozlišovat mezi prostory, které jsou navzájem izomorfní.

**Věta 9.4** *Jsou-li $\mathcal{V}$ a $\mathcal{V}'$ vektorové prostory nad $\mathcal{T}$, je-li $f$ izomorfizmus $\mathcal{V}$ na $\mathcal{V}'$ a je-li $\{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ báze prostoru $\mathcal{V}$, pak množina $\{f(\overrightarrow{u_1}), \dots, f(\overrightarrow{u_n})\}$ je bází prostoru $\mathcal{V}'$.*

D ů k a z: Ukažme nejdříve, že $\{f(\overrightarrow{u_1}), \dots, f(\overrightarrow{u_n})\}$ je množina generátorů vektorového prostoru $\mathcal{V}'$. Nechť $\overrightarrow{u}' \in \mathcal{V}'$. Protože $f$ je surjektivní, existuje $\overrightarrow{u} \in \mathcal{V}$ takový, že $f(\overrightarrow{u}) = \overrightarrow{u}'$. Podle předpokladu platí $[\{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}] = \mathcal{V}$, proto existují $c_1, \dots, c_n \in T$ tak, že

$$\overrightarrow{u} = \sum_{i=1}^{n} c_i \overrightarrow{u_i}.$$

Potom

$$\overrightarrow{u}' = f(\overrightarrow{u}) = f\left(\sum_{i=1}^{n} c_i \overrightarrow{u_i}\right) = \sum_{i=1}^{n} c_i f(\overrightarrow{u_i}),$$

tedy $[\{f(\overrightarrow{u_1}), \dots, f(\overrightarrow{u_n})\}] = \mathcal{V}'$.

Zbývá dokázat, že množina $\{f(\overrightarrow{u_1}), \dots, f(\overrightarrow{u_n})\}$ je lineárně nezávislá. Nechť $d_1, \dots, d_n \in T$ jsou taková čísla, že

$$\sum_{i=1}^{n} d_i f(\overrightarrow{u_i}) = \overrightarrow{o}'.$$

Pak

$$\overrightarrow{o}' = f\left(\sum_{i=1}^{n} d_i \overrightarrow{u_i}\right),$$

a protože podle věty 9.1 Ker$f = \{\overrightarrow{o}\}$, platí

$$\sum_{i=1}^{n} d_i \overrightarrow{u_i} = \overrightarrow{o}.$$

Z lineární nezávislosti vektorů $\overrightarrow{u_1}, \dots, \overrightarrow{u_n}$ dostáváme $d_1 = \dots = d_n = 0$, proto jsou také vektory $f(\overrightarrow{u_1}), \dots, f(\overrightarrow{u_n})$ lineárně nezávislé. □

V následujících příkladech budeme zkoumat zobrazení kartézských mocnin množiny reálných čísel $\mathbb{R}$ do dalších kartézských mocnin množiny $\mathbb{R}$. Naším úkolem bude ověřit, že každé z těchto zobrazení je homomorfizmem příslušných aritmetických vektorových prostorů nad $\mathcal{R}$, a dále budeme zjišťovat, zda jsou tyto homomorfizmy injektivní, surjektivní, popř. jsou-li izomorfizmy.

**Příklad 9.1** Uvažujme zobrazení $f : \mathcal{R}^2 \to \mathcal{R}^2$ takové, že pro každý vektor $(x_1, x_2) \in \mathcal{R}^2$ platí $f((x_1, x_2)) = (2x_1 + x_2, x_1 + x_2)$.

Pro libovolné $(x_1, x_2), (y_1, y_2) \in \mathcal{R}^2$ a $c \in \mathcal{R}$ platí $f((x_1, x_2) + (y_1, y_2)) = f((x_1 + y_1, x_2 + y_2)) = (2(x_1 + y_1) + (x_2 + y_2), (x_1 + y_1) + (x_2 + y_2)) = ((2x_1 + x_2) + (2y_1 + y_2), (x_1 + x_2) + (y_1 + y_2)) = (2x_1 + x_2, x_1 + x_2) + (2y_1 + y_2, y_1 + y_2) = f((x_1, x_2)) + f((y_1 y_2))$, $f(c(x_1, x_2)) = f((cx_1, cx_2)) = (2cx_1 + cx_2, cx_1 + cx_2) = c(2x_1 + x_2, x_1 + x_2) = cf((x_1, x_2))$, tedy $f$ je homomorfizmus $\mathcal{R}^2$ do $\mathcal{R}^2$.

Nechť $(x_1, x_2) \in \mathcal{R}^2$ je takový vektor, že $f((x_1, x_2)) = \overrightarrow{o}$, tj. platí

$$2x_1 + x_2 = 0, \quad x_1 + x_2 = 0.$$

Potom $x_1 = x_2 = 0$, tedy $(x_1, x_2) = \overrightarrow{o}$, a to znamená, že $\mathrm{Ker} f = \{\overrightarrow{o}\}$, neboli že $f$ je injektivní.

Ukážeme ještě, že pro každý vektor $(y_1, y_2) \in \mathcal{R}^2$ existuje $(x_1, x_2) \in \mathcal{R}^2$, který je jeho vzorem v homomorfizmu $f$. Pro takový $(x_1, x_2)$ musí platit $f((x_1, x_2)) = (y_1, y_2)$, tedy

$$y_1 = 2x_1 + x_2, \quad y_2 = x_1 + x_2.$$

Odtud dostáváme

$$x_1 = y_1 - y_2, \quad x_2 = 2y_2 - y_1,$$

a snadno se přesvědčíme, že opravdu platí $(y_1, y_2) = f(y_1 - y_2, 2y_2 - y_1)$. Homomorfizmus je tedy surjektivní.

Celkově proto dostáváme, že $f$ je izomorfizmem $\mathcal{R}^2$ na $\mathcal{R}^2$.

**Příklad 9.2** Označme $g$ zobrazení $\mathcal{R}^3$ do $\mathcal{R}^4$ takové, že pro každý vektor $(x_1, x_2, x_3) \in \mathcal{R}^3$ platí $g((x_1, x_2, x_3)) = (x_1, x_1, x_2, x_3)$.

Podobně jako v příkladu 9.1 snadno dokážeme, že $g$ je homomorfizmus $\mathcal{R}^3$ do $\mathcal{R}^4$.

Jestliže pro $(x_1, x_2, x_3) \in \mathcal{R}^3$ platí $g((x_1, x_2, x_3)) = \overrightarrow{o}$, pak $x_1 = x_2 = x_3 = 0$, tedy $(x_1, x_2, x_3) = \overrightarrow{o}$. To znamená, že $\mathrm{Ker} f = \{\overrightarrow{o}\}$, neboli že $g$ je injektivní.

Dále platí, že $\mathrm{Im} g = \{(x_1, x_1, x_2, x_3); (x_1, x_2, x_3) \in \mathcal{R}^3\}$, tedy $\mathrm{Im} g$ je vlastní podmnožinou $\mathcal{R}^4$. Proto $g$ není surjektivní, což znamená, že není ani izomorfizmus.

**Příklad 9.3** Uvažujme zobrazení $h : \mathcal{R}^2 \to \mathcal{R}$ takové, že $h((x_1, x_2)) = (x_1 + x_2)$.

Přímým výpočtem můžeme ověřit, že $h$ je homomorfizmus $\mathcal{R}^2$ do $\mathcal{R}$.

Jestliže pro $(x_1, x_2) \in \mathcal{R}^2$ platí $h((x_1, x_2)) = \overrightarrow{o}$, pak $x_1 + x_2 = 0$, neboli $\mathrm{Ker} h = \{(x_1, x_2) \in \mathcal{R}^2; x_1 = -x_2\}$, a tedy $h$ není injektivní, proto není ani izomorfizmem.

Homomorfizmus $h$ je ale surjektivní, protože pro každý $x \in \mathcal{R}$ platí $(x) = h((x, 0))$.

## 9.2 Transformace souřadnic

**Definice 9.4** *Nechť $\mathcal{V}$ je vektorový prostor nad $\mathcal{T}$ takový, že $\dim \mathcal{V} = n$. Je-li $M = \{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ báze prostoru $\mathcal{V}$ a*

$$\overrightarrow{u} = \sum_{i=1}^{n} c_i \overrightarrow{u_i}$$

*vektor z $\mathcal{V}$, potom koeficienty $c_1, \dots, c_n$ nazýváme* souřadnice vektoru $\overrightarrow{u}$ vzhledem k bázi $M$ *a píšeme*

$$\{\overrightarrow{u}\}_M = (c_1, \dots, c_n).$$

**Věta 9.5** *Je-li $M = \{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ báze prostoru $\mathcal{V}$ a jsou-li $\overrightarrow{u}, \overrightarrow{v} \in V$, $c \in T$, pak*

$$\{\overrightarrow{u} + \overrightarrow{v}\}_M = \{\overrightarrow{u}\}_M + \{\overrightarrow{v}\}_M, \{c\overrightarrow{u}\}_M = c\{\overrightarrow{u}\}_M.$$

D ů k a z: Nechť $\{\overrightarrow{u}\}_M = (c_1, \dots, c_n)$, $\{\overrightarrow{v}\}_M = (d_1, \dots, d_n)$. Pak

$$\overrightarrow{u} = \sum_{i=1}^{n} c_i \overrightarrow{u_i}, \overrightarrow{v} = \sum_{i=1}^{n} d_i \overrightarrow{u_i},$$

proto

$$\overrightarrow{u} + \overrightarrow{v} = \sum_{i=1}^{n} (c_i + d_i) \overrightarrow{u_i}, c\overrightarrow{u} = \sum_{i=1}^{n} (cc_i) \overrightarrow{u_i}.$$

□

**Věta 9.6** *Jestliže $M = \{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ je báze vektorového prostoru $\mathcal{V}$ dimenze $n$ nad $\mathcal{T}$, potom zobrazení $f : V \to T^n$ takové, že pro každý vektor $\overrightarrow{u} \in V$ platí $f(\overrightarrow{u}) = \{\overrightarrow{u}\}_M$ je izomorfizmem vektorového prostoru $\mathcal{V}$ na aritmetický vektorový prostor $\mathcal{T}^n$.*

D ů k a z: Nechť $\overrightarrow{u}, \overrightarrow{v} \in V$, $c \in T$. Pak

$$f(\overrightarrow{u} + \overrightarrow{v}) = \{\overrightarrow{u} + \overrightarrow{v}\}_M = \{\overrightarrow{u}\}_M + \{\overrightarrow{v}\}_M = f(\overrightarrow{u}) + f(\overrightarrow{v}),$$

$$f(c\overrightarrow{u}) = \{c\overrightarrow{u}\}_M = c\{\overrightarrow{u}\}_M = cf(\overrightarrow{u}),$$

tedy $f$ je homomorfizmus $\mathcal{V}$ do $\mathcal{T}^n$.

Je-li $f(\overrightarrow{u}) = \overrightarrow{o}$, potom $\{\overrightarrow{u}\}_M = \overrightarrow{o}$, což znamená

$$\overrightarrow{u} = \sum_{i=1}^{n} 0\overrightarrow{u_i} = \overrightarrow{o}.$$

Platí tedy $\mathrm{Ker} f = \{\overrightarrow{o}\}$, a proto $f$ je injektivní.

Jestliže $(c_1, \dots, c_n) \in T^n$, pak

$$(c_1, \dots, c_n) = f\left(\sum_{i=1}^{n} c_i \overrightarrow{u_i}\right),$$

tedy $f$ je surjektivní. □

**Věta 9.7** *Každý vektorový prostor nad $\mathcal{T}$ dimenze $n$ je izomorfní s aritmetickým vektorovým prostorem $\mathcal{T}^n$.*

D ů k a z: Tvrzení je přímým důsledkem věty 9.6. □

**Věta 9.8** *Dva vektorové prostory $\mathcal{V}$ a $\mathcal{V}'$ konečné dimenze nad $\mathcal{T}$ jsou izomorfní právě tehdy, mají-li stejnou dimenzi.*

D ů k a z: Nechť $\dim \mathcal{V} = \dim \mathcal{V}' = n$. Pak existují podle věty 9.7 izomorfizmy $f : \mathcal{V} \to \mathcal{T}^n$ a $g : \mathcal{V}' \to \mathcal{T}^n$. Protože podle věty 9.3 je $g^{-1}$ izomorfizmus $\mathcal{T}^n$ na $\mathcal{V}'$, je $f \circ g^{-1}$ izomorfizmem $\mathcal{V}$ na $\mathcal{V}'$.

Obráceně, nechť $f$ je izomorfizmus $\mathcal{V}$ na $\mathcal{V}'$. Je-li $\{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ báze prostoru $\mathcal{V}$, pak podle věty 9.4 je $\{f(\overrightarrow{u_1}), \dots, f(\overrightarrow{u_n})\}$ báze prostoru $\mathcal{V}'$, tedy $\dim \mathcal{V} = \dim \mathcal{V}'$. □

**Definice 9.5** *Nechť $M = \{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ a $M' = \{\overrightarrow{u_1}', \dots, \overrightarrow{u_n}'\}$ jsou dvě báze vektorového prostoru $\mathcal{V}$ a nechť $\{\overrightarrow{u_i}'\}_M = (a_{i1}, a_{i2}, \dots, a_{in})$, $i = 1, \dots, n$. Potom matici $A = ||a_{ij}||$ nazýváme* maticí přechodu od báze $M$ k bázi $M'$.

**Věta 9.9** *Nechť $M = \{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ a $M' = \{\overrightarrow{u_1}', \dots, \overrightarrow{u_n}'\}$ jsou báze vektorového prostoru $\mathcal{V}$ a nechť $A$ je matice přechodu od báze $M$ k bázi $M'$. Potom pro každý vektor $\overrightarrow{u} \in V$ platí*

$$\{\overrightarrow{u}\}_M = \{\overrightarrow{u}\}_{M'} \cdot A.$$

D ů k a z: Nechť $A = ||a_{ij}||$, $\{\overrightarrow{u}\}_M = (c_1, \dots, c_n)$, $\{\overrightarrow{u}\}_{M'} = (c_1', \dots, c_n')$. Potom

$$\overrightarrow{u} = \sum_{i=1}^{n} c_i \overrightarrow{u_i} = \sum_{j=1}^{n} c_j' \overrightarrow{u_j}' \quad \text{a} \quad \overrightarrow{u_j}' = \sum_{i=1}^{n} a_{ji} \overrightarrow{u_i}.$$

Tedy

$$\overrightarrow{u} = \sum_{j=1}^{n} c_j' \overrightarrow{u_j}' = \sum_{j=1}^{n} c_j' \sum_{i=1}^{n} a_{ji} \overrightarrow{u_i} = \sum_{i=1}^{n} \left( \sum_{j=1}^{n} c_j' a_{ji} \right) \overrightarrow{u_i}.$$

Protože vektor $\overrightarrow{u}$ je možno vyjádřit právě jedním způsobem ve tvaru lineární kombinace vektorů báze $M$, dostáváme z rovnosti

$$\sum_{i=1}^{n} c_i \overrightarrow{u_i} = \sum_{i=1}^{n} \left( \sum_{j=1}^{n} c_j' a_{ji} \right) \overrightarrow{u_i},$$

že

$$c_i = \sum_{j=1}^{n} c_j' a_{ji},$$

pro každé $i = 1, \dots, n$. To ovšem znamená, že

$$(c_1, \dots, c_n) = (c_1', \dots, c_n') \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix},$$

tedy $\{\overrightarrow{u}\}_M = \{\overrightarrow{u}\}_{M'} A$. □

**Věta 9.10** *Jestliže* $M = \{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$, $M' = \{\overrightarrow{u_1}', \dots, \overrightarrow{u_n}'\}$ *a* $M'' = \{\overrightarrow{u}'', \dots, \overrightarrow{u_n}''\}$ *jsou báze vektorového prostoru* $\mathcal{V}$, $A = ||a_{ij}||$ *je matice přechodu od* $M$ *k* $M'$ *a* $B = ||b_{ij}||$ *je matice přechodu od* $M'$ *k* $M''$, *pak* $BA$ *je matice přechodu od* $M$ *k* $M''$.

D ů k a z: Platí

$$\overrightarrow{u_k}' = \sum_{j=1}^{n} a_{kj}\overrightarrow{u_j}, k = 1, \dots, n,$$

$$\overrightarrow{u_i}'' = \sum_{k=1}^{n} b_{ik}\overrightarrow{u_k}', i = 1, \dots, n.$$

Tedy

$$\overrightarrow{u_i}'' = \sum_{k=1}^{n} b_{ik}\overrightarrow{u_k}' = \sum_{k=1}^{n} b_{ik}\sum_{j=1}^{n} a_{kj}\overrightarrow{u_j} = \sum_{j=1}^{n}\left(\sum_{k=1}^{n} b_{ik}a_{kj}\right)\overrightarrow{u_j} = \sum_{j=1}^{n} c_{ij}\overrightarrow{u_j},$$

kde

$$c_{ij} = \sum_{k=1}^{n} b_{ik}a_{kj},$$

proto matice $C = ||c_{ij}||$, která je maticí přechodu od $M$ k $M''$, je rovna matici $BA$. □

**Věta 9.11** *Jestliže* $M = \{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ *a* $M' = \{\overrightarrow{u_1}', \dots, \overrightarrow{u_n}'\}$ *jsou báze vektorového prostoru* $\mathcal{V}$ *a je-li* $A$ *matice přechodu od* $M$ *k* $M'$, *potom platí, že matice* $A$ *je regulární a že* $A^{-1}$ *je maticí přechodu od* $M'$ *k* $M$.

D ů k a z: Je zřejmé, že matice přechodu od kterékoliv báze k téže bázi je jednotková. Označme $B$ matici přechodu od $M'$ k $M$. Potom podle věty 9.10 platí $BA = AB = E$, tedy $B = A^{-1}$. □

**Věta 9.12** *Nechť* $M = \{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ *je báze vektorového prostoru* $\mathcal{V}$. *Je-li* $A = ||a_{ij}||$ *regulární čtvercová matice stupně* $n$, *potom množina* $M' = \{\overrightarrow{u_1}', \dots, \overrightarrow{u_n}'\}$ *kde*

$$\overrightarrow{u_i}' = \sum_{j=1}^{n} a_{ij}\overrightarrow{u_j}, i = 1, \dots, n,$$

*je bází prostoru* $\mathcal{V}$ *a* $A$ *je maticí přechodu od* $M$ *k* $M'$.

D ů k a z: Ukažme, že vektory $\overrightarrow{u_1}', \dots, \overrightarrow{u_n}'$ jsou lineárně nezávislé. Nechť

$$\sum_{i=1}^{n} c_i\overrightarrow{u_i}' = \overrightarrow{o}.$$

Potom

$$\sum_{i=1}^{n} c_i \sum_{j=1}^{n} a_{ij} \overrightarrow{u_j} = \sum_{j=1}^{n} \left( \sum_{i=1}^{n} c_i a_{ij} \right) \overrightarrow{u_j} = \overrightarrow{o}.$$

Protože množina $M$ je lineárně nezávislá, platí

$$\sum_{i=1}^{n} c_i a_{ij} = 0, \text{ pro každé } j = 1, \ldots, n.$$

Označme $A^{-1} = ||b_{ij}||$ a vynásobme každou z rovností

$$\sum_{i=1}^{n} c_i a_{ij} = 0$$

prvkem $b_{jk}$ matice $A^{-1}$ $(j = 1, \ldots, n)$. Vzniklé rovnosti sečteme a dostaneme

$$0 = \sum_{j=1}^{n} \sum_{i=1}^{n} c_i a_{ij} b_{jk} = \sum_{i=1}^{n} c_i \sum_{j=1}^{n} a_{ij} b_{jk}.$$

Víme, že součin $i$-tého řádku matice $A$ s $k$-tým sloupcem inverzní matice $A^{-1}$ je roven 1 pro $i = k$ a je roven 0 pro $i \neq k$. Proto dostáváme

$$\sum_{i=1}^{n} c_i \sum_{j=1}^{n} a_{ij} b_{jk} = c_k,$$

a tedy $c_k = 0$. Protože $k$ je kterékoliv číslo z množiny $\{1, \ldots, n\}$, platí $c_1 = \ldots = c_n = 0$, a proto jsou vektory $\overrightarrow{u_1}', \ldots, \overrightarrow{u_n}'$ lineárně nezávislé.

Skutečnost, že $[M'] = \mathcal{V}$, dokazovat nemusíme, protože podle věty 6.15 je každá $n$-prvková lineárně nezávislá množina vektorového prostoru dimenze $n$ bází tohoto prostoru.□

**Příklad 9.4**

a) Určete matici přechodu od báze $M = \{\overrightarrow{u_1}, \overrightarrow{u_2}, \overrightarrow{u_3}\} = \{(2,3,1), (0,1,2), (1,2,1)\}$ k bázi $M' = \{\overrightarrow{u_1}', \overrightarrow{u_2}', \overrightarrow{u_3}'\} = \{(3,5,2), (6,11,6), (-1,1,4)\}$ vektorového prostoru $\mathcal{R}^3$.

b) Určete vztah mezi souřadnicemi libovolného vektoru $\overrightarrow{u} \in \mathcal{R}^3$ vzhledem k bázím $M$ a $M'$.

K řešení použijeme předchozích vět:

a) Nechť $\{\overrightarrow{u_i}'\}_M = (a_{i1}, a_{i2}, a_{i3})$, $i = 1, 2, 3$. Pak

$$\overrightarrow{u_i}' = \sum_{j=1}^{3} a_{ij} \overrightarrow{u_j}.$$

Budeme tedy řešit 3 soustavy rovnic o 3 neznámých. Vzhledem k tomu, že matice soustav jsou stejné, můžeme řešit všechny tři soustavy najednou. K zápisu použijeme rozšířenou matici se třemi pravými stranami.

$$\left(\begin{array}{ccc|c|c|c} 2 & 0 & 1 & 3 & 6 & -1 \\ 3 & 1 & 2 & 5 & 11 & 1 \\ 1 & 2 & 1 & 2 & 6 & 4 \end{array}\right) \overset{\check{r}}{\sim} \left(\begin{array}{ccc|c|c|c} 1 & 2 & 1 & 2 & 6 & 4 \\ 0 & -4 & -1 & -1 & -6 & -9 \\ 0 & -5 & -1 & -1 & -7 & -11 \end{array}\right) \overset{\check{r}}{\sim}$$

$$\overset{\check{r}}{\sim} \left(\begin{array}{ccc|c|c|c} 1 & 2 & 1 & 2 & 6 & 4 \\ 0 & 4 & 1 & 1 & 6 & 9 \\ 0 & 1 & 0 & 0 & 1 & 2 \end{array}\right).$$

Odtud dostáváme

$$\begin{array}{lll} a_{11} = 1, & a_{12} = 0, & a_{13} = 1, \\ a_{21} = 2, & a_{22} = 1, & a_{23} = 2, \\ a_{31} = -1, & a_{32} = 2, & a_{33} = 1. \end{array}$$

Tedy

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

je maticí přechodu od $M$ k $M'$.

b) Víme, že maticí přechodu od $M'$ k $M$ je inverzní matice $A^{-1}$ k matici $A$. Určeme tedy nejdříve $A^{-1}$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 2 & 1 & 2 & 0 & 1 & 0 \\ -1 & 2 & 1 & 0 & 0 & 1 \end{array}\right) \overset{\check{r}}{\sim} \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & -2 & 1 & 0 \\ 0 & 2 & 2 & 1 & 0 & 1 \end{array}\right) \overset{\check{r}}{\sim}$$

$$\overset{\check{r}}{\sim} \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & -2 & 1 & 0 \\ 0 & 0 & 2 & 5 & -2 & 1 \end{array}\right) \overset{\check{r}}{\sim} \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & -2 & 1 & 0 \\ 0 & 0 & 1 & \frac{5}{2} & -1 & \frac{1}{2} \end{array}\right) \overset{\check{r}}{\sim}$$

$$\overset{\check{r}}{\sim} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{3}{2} & 1 & -\frac{1}{2} \\ 0 & 1 & 0 & -2 & 1 & 0 \\ 0 & 0 & 1 & \frac{5}{2} & -1 & \frac{1}{2} \end{array}\right).$$

Tedy

$$A^{-1} = \begin{pmatrix} -\frac{3}{2} & 1 & -\frac{1}{2} \\ -2 & 1 & 0 \\ \frac{5}{2} & -1 & \frac{1}{2} \end{pmatrix}.$$

Je-li $\overrightarrow{u} \in \mathcal{R}^3$, označme $\{\overrightarrow{u}\}_M = (x_1, x_2, x_3)$, $\{\overrightarrow{u}\}_{M'} = (x'_1, x'_2, x'_3)$. Pak platí

$$(x_1, x_2, x_3) = (x'_1, x'_2, x'_3) \begin{pmatrix} 1 & 0 & 1 \\ 2 & 1 & 2 \\ -1 & 2 & 1 \end{pmatrix},$$

tedy

$$\begin{aligned} x_1 &= x_1' + 2x_2' - x_3, \\ x_2 &= x_2' + 2x_3', \\ x_3 &= x_1' + 2x_2' + x_3'. \end{aligned}$$

Podobně

$$(x_1', x_2', x_3') = (x_1, x_2, x_3) \begin{pmatrix} -\frac{3}{2} & 1 & -\frac{1}{2} \\ -2 & 1 & 0 \\ \frac{5}{2} & -1 & \frac{1}{2} \end{pmatrix},$$

tedy

$$\begin{aligned} x_1' &= -\tfrac{3}{2}x_1 - 2\xi_2 + \tfrac{5}{2}x_3, \\ x_2' &= x_1 + \xi_2 - x_3, \\ x_3' &= -\tfrac{1}{2}x_1 + \tfrac{1}{2}x_3. \end{aligned}$$

## 9.3 Cvičení

**9.1** Rozhodněte, která z následujících zobrazení jsou homomorfizmy příslušných aritmetických vektorových prostorů. V případě homomorfizmů zjistěte, jsou-li injektivní, surjektivní, popř. jsou-li to izomorfizmy.

a) $f : \mathcal{R}^4 \to \mathcal{R}^2$, $f((x_1, x_2, x_3, x_4)) = (x_2, x_3)$;

b) $g : \mathcal{R}^3 \to \mathcal{R}^2$, $f((x_1, x_2, x_3)) = (x_1, x_2^3)$;

c) $h : \mathcal{R}^2 \to \mathcal{R}^2$, $f((x_1, x_2)) = (x_1 + 3x_2, 2x_1 - x_2)$.

[ a) surjektivní homomorfizmus; b) není; c) izomorfizmus ]

**9.2** Nechť jsou dány báze $M = \{(2, -1), (1, -3)\}$, $M' = \{(-5, 0), (-6, -2)\}$ a $M'' = \{(2, 4), (7, 4)\}$ prostoru $\mathcal{R}^2$. Určete matici přechodu

a) od báze $M$ k bázi $M'$;

b) od báze $M'$ k bázi $M''$;

c) od báze $M$ k bázi $M''$.

[ a) $\begin{pmatrix} -3 & 1 \\ -4 & 2 \end{pmatrix}$; b) $\begin{pmatrix} 2 & -2 \\ 1 & -2 \end{pmatrix}$; c) $\begin{pmatrix} 2 & -2 \\ 5 & -3 \end{pmatrix}$ ]

**9.3** Určete vztahy mezi souřadnicemi libovolného vektoru $\overrightarrow{u} \in \mathcal{R}^3$ vzhledem k bázím $M = \{(1, 2, -1), (-2, 1, 0), (-2, 1, 1)\}$ a $M' = \{(0, 5, -1), (5, 0, -1), (-4, 2, 1)\}$ prostoru $\mathcal{R}^3$. ($\{\overrightarrow{u}\}_M = (x_1, x_2, x_3)$, $\{\overrightarrow{u}\}_{M'} = (x_1', x_2', x_3')$.)

$$\left[ \begin{array}{llll} x_1 = & 2x_1' + x_2' & x_1' = & \frac{2}{3}x_1 + \frac{1}{3}x_2 - \frac{1}{3}x_3 \\ x_2 = & -2x_2' + x_3', & x_2' = & -\frac{1}{3}x_1 - \frac{2}{3}x_2 + \frac{2}{3}x_3. \\ x_3 = & x_1' + x_3' & x_3' = & -\frac{2}{3}x_1 - \frac{1}{3}x_2 + \frac{4}{3}x_3 \end{array} \right]$$

# Kapitola 10

# Eukleidovské vektorové prostory

## 10.1 Definice a základní vlastnosti

Definice vektorového prostoru nad číselným tělesem $\mathcal{T}$, která je založena na operaci sčítání vektorů a na vnější operaci násobení vektorů skaláry, umožňuje zavést pojmy lineárně závislých a nezávislých vektorů a pojem dimenze vektorového prostoru. Víme, že tyto pojmy jsou invariantní vzhledem k izomorfizmům vektorových prostorů. Základními příklady vektorových prostorů jsou však aritmetické vektorové prostory, ve kterých je možno navíc velice jednoduchým způsobem definovat délku vektorů a úhel mezi vektory. Připomeňme si to např. pro aritmetický vektorový prostor $\mathcal{R}^2$.

Jsou-li $\overrightarrow{u} = (u_1, u_2)$ a $\overrightarrow{v} = (v_1, v_2)$ vektory z $\mathcal{R}^2$, označme

$$\langle \overrightarrow{u}, \overrightarrow{v} \rangle = u_1 v_1 + u_2 v_2.$$

Je zřejmé, že $\langle \overrightarrow{u}, \overrightarrow{v} \rangle$ je reálné číslo. Toto číslo se nazývá skalárním součinem vektorů $\overrightarrow{u}$ a $\overrightarrow{v}$. Víme, že v analytické geometrii je délka $||\overrightarrow{u}||$ definována jako číslo

$$||\overrightarrow{u}|| = \sqrt{u_1^2 + u_2^2}.$$

Platí tedy, že

$$||\overrightarrow{u}|| = \sqrt{\langle \overrightarrow{u}, \overrightarrow{u} \rangle}$$

a že pro úhel $\varphi$ dvou nenulových vektorů $\overrightarrow{u}, \overrightarrow{v}$ je

$$\cos\varphi = \frac{\langle \overrightarrow{u}, \overrightarrow{v} \rangle}{\sqrt{\langle \overrightarrow{u}, \overrightarrow{u} \rangle \langle \overrightarrow{v}, \overrightarrow{v} \rangle}}.$$

(To ovšem znamená, že vektory $\overrightarrow{u}$ a $\overrightarrow{v}$ jsou pak navzájem kolmé (neboli ortogonální) právě tehdy, platí-li $\langle \overrightarrow{u}, \overrightarrow{v} \rangle = 0$.)

Pro tyto výsledky však bylo podstatné, že bází prostoru $\mathcal{R}^2$ byla množina $\{\overrightarrow{e_1}, \overrightarrow{e_2}\}$, kde $\overrightarrow{e_1} = (1, 0), \overrightarrow{e_2} = (0, 1)$. Přitom však platí, že je-li $f : \mathcal{R}^2 \to \mathcal{R}^2$ takové zobrazení, že pro každý vektor $\overrightarrow{u} = (u_1, u_2) \in \mathcal{R}^2$

$$f(\overrightarrow{u}) = (2u_1, 2u_2) = 2\overrightarrow{u},$$

pak $f$ je izomorfizmem $\mathcal{R}^2$ na $\mathcal{R}^2$, ale délka vektoru $f(\overrightarrow{u})$ je rovna číslu $2||\overrightarrow{u}||$, tedy pro izomorfizmus vektorových prostorů může platit, že délka vektoru je různá od délky jeho obrazu.

Podobně izomorfizmus vektorových prostorů nemusí zachovávat ani velikost úhlů mezi vektory. Např. regulární matice

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

je maticí přechodu od báze $\{\overrightarrow{e_1}, \overrightarrow{e_2}\}$ k bázi $\{\overrightarrow{e_1}', \overrightarrow{e_2}'\}$, kde $\overrightarrow{e_1}' = (1, 2)$, $\overrightarrow{e_2}' = (0, -1)$, a tedy určuje izomorfizmus $f : \mathcal{R}^2 \to \mathcal{R}^2$, pro který mj. platí $f(\overrightarrow{e_1}) = \overrightarrow{e_1}'$, $f(\overrightarrow{e_2}) = \overrightarrow{e_2}'$.

Přitom ale

$$\langle \overrightarrow{e_1'}, \overrightarrow{e_2'} \rangle = 1 \cdot 0 + 2 \cdot (-1) = -2,$$

tedy kolmé vektory $\overrightarrow{e_1}$ a $\overrightarrow{e_2}$ se zobrazí na vektory $\overrightarrow{e_1'}$ a $\overrightarrow{e_2'}$, které nejsou kolmé.

Je tedy zřejmé, že chceme-li obecně definovat pojmy délky vektoru a úhlu dvou vektorů, musíme strukturu vektorových prostorů dále rozšířit. Přitom se omezíme na vektorové prostory nad tělesem reálných čísel $\mathcal{R}$.

**Definice 10.1** Eukleidovský vektorový prostor *je každý vektorový prostor $\mathcal{E}$ nad tělesem $\mathcal{R}$ uvažovaný spolu se zobrazením $g : E \times E \to \mathbb{R}$, pro které platí:*

1. $\forall \overrightarrow{u}, \overrightarrow{v} \in E;\ g(\overrightarrow{u}, \overrightarrow{v}) = g(\overrightarrow{v}, \overrightarrow{u})$,
2. $\forall \overrightarrow{u}, \overrightarrow{v}, \overrightarrow{w} \in E;\ g(\overrightarrow{u} + \overrightarrow{v}, \overrightarrow{w}) = g(\overrightarrow{u}, \overrightarrow{w}) + g(\overrightarrow{v}, \overrightarrow{w})$,
3. $\forall c \in \mathbb{R}, \overrightarrow{u}, \overrightarrow{v} \in E;\ g(c\overrightarrow{u}, \overrightarrow{v}) = cg(\overrightarrow{u}, \overrightarrow{v})$,
4. $\forall \overrightarrow{o} \neq \overrightarrow{u} \in E;\ g(\overrightarrow{u}, \overrightarrow{u}) > 0.$,

*Zobrazení $g$ budeme nazývat* skalární součin. *Eukleidovský prostor $\mathcal{E}$ se skalárním součinem $g$ označíme $(\mathcal{E}, g)$.*

Bude-li zřejmé, který skalární součin uvažujeme, budeme místo $g(\overrightarrow{u}, \overrightarrow{v})$ psát zkráceně $\langle \overrightarrow{u}, \overrightarrow{v} \rangle$ a místo označení $(\mathcal{E}, g)$ použijeme také stručnější $\mathcal{E}$.

**Příklad 10.1** Je-li $n \in \mathbb{N}$, pak v aritmetickém vektorovém prostoru $\mathcal{R}^n$ můžeme zavést skalární součin $g$ tak, že pro libovolné vektory $\overrightarrow{u} = (u_1, u_2, \ldots, u_n)$, $\overrightarrow{v} = (v_1, v_2, \ldots, v_n)$ položíme

$$\langle \overrightarrow{u}, \overrightarrow{v} \rangle = \sum_{i=1}^{n} u_i v_i.$$

Tomuto skalárnímu součinu budeme také říkat *„obyčejný skalární součin"*.

**Příklad 10.2** Označme $C[0,1]$ množinu všech spojitých reálných funkcí definovaných na intervalu $[0,1]$. Potom $C = C[0,1]$ spolu se sčítáním funkcí a s násobením funkcí reálnými čísly tvoří vektorový prostor $\mathcal{C}$, který není konečné dimenze. Pro libovolné funkce $\varphi, \psi \in C$ položme

$$\langle \varphi, \psi \rangle = \int_0^1 \varphi(x)\psi(x)dx.$$

Můžeme se snadno přesvědčit, že takto definované zobrazení $C \times C \to \mathbb{R}$ je skalárním součinem.

**Definice 10.2** *Je-li $\mathcal{E}$ eukleidovský vektorový prostor, $\overrightarrow{u} \in E$, pak* délkou vektoru $\overrightarrow{u}$ *budeme rozumět číslo*

$$||\overrightarrow{u}|| = \sqrt{\langle \overrightarrow{u}, \overrightarrow{u} \rangle}.$$

**Věta 10.1** *V eukleidovském prostoru $\mathcal{E}$ platí*

*a)* $\forall c \in \mathbb{R}, \overrightarrow{u} \in E$; $||c\overrightarrow{u}|| = |c| \cdot ||\overrightarrow{u}||$,

*b)* $\forall \overrightarrow{u} \in E, \overrightarrow{u} \neq \overrightarrow{o}$; $||\overrightarrow{u}|| > 0$,

*c)* $\forall \overrightarrow{u}, \overrightarrow{v} \in E$; $|\langle \overrightarrow{u}, \overrightarrow{v} \rangle| \leq ||\overrightarrow{u}|| \cdot ||\overrightarrow{v}||$ *(Schwarzova nerovnost),*

*d)* $\forall \overrightarrow{u}\,\overrightarrow{v} \in E$; $||\overrightarrow{u} + \overrightarrow{v}|| \leq ||\overrightarrow{u}|| + ||\overrightarrow{v}||$ *(trojúhelníková nerovnost).*

D ů k a z:

a) Platí $\langle c\overrightarrow{u}, c\overrightarrow{u} \rangle = c^2 \langle \overrightarrow{u}, \overrightarrow{u} \rangle$, proto $||c\overrightarrow{u}|| = |c| \cdot ||\overrightarrow{u}||$.

b) Plyne přímo z podmínky 4 z definice eukleidovského vektorového prostoru.

c) Pro $\overrightarrow{u} = \overrightarrow{o}$ nebo $\overrightarrow{v} = \overrightarrow{o}$ dostáváme pravdivou nerovnost $0 \leq 0$. Předpokládejme v dalším, že $\overrightarrow{u} \neq \overrightarrow{o}$ a $\overrightarrow{v} \neq \overrightarrow{o}$. Potom pro libovolné $c \in \mathbb{R}$ platí

$$\langle \overrightarrow{u} - c\overrightarrow{v}, \overrightarrow{u} - c\overrightarrow{v} \rangle \geq 0,$$

to znamená, že použitím definice eukleidovského vektorového prostoru dostaneme

$$0 \leq \langle \overrightarrow{u} - c\overrightarrow{v}, \overrightarrow{u} - c\overrightarrow{v} \rangle = \langle \overrightarrow{u}, \overrightarrow{u} - c\overrightarrow{v} \rangle + \langle -c\overrightarrow{v}, \overrightarrow{u} - c\overrightarrow{v} \rangle =$$

$$= \langle \overrightarrow{u}, \overrightarrow{u} \rangle + \langle \overrightarrow{u}, -c\overrightarrow{v} \rangle + \langle -c\overrightarrow{v}, \overrightarrow{u} \rangle + \langle -c\overrightarrow{v}, -c\overrightarrow{v} \rangle =$$

$$= \langle \overrightarrow{u}, \overrightarrow{u} \rangle - c\langle \overrightarrow{u}, \overrightarrow{v} \rangle - c\langle \overrightarrow{u}, \overrightarrow{v} \rangle + c^2 \langle \overrightarrow{v}, \overrightarrow{v} \rangle,$$

tedy platí

$$c^2 \langle \overrightarrow{v}, \overrightarrow{v} \rangle - 2c\langle \overrightarrow{u}, \overrightarrow{v} \rangle + \langle \overrightarrow{u}, \overrightarrow{u} \rangle \geq 0.$$

Výraz na levé straně můžeme uvažovat jako kvadratický trojčlen vzhledem k $c$. Tento trojčlen nemůže mít dva různé reálné kořeny, proto pro jeho diskriminant platí

$$4\langle \overrightarrow{u}, \overrightarrow{v} \rangle^2 - 4\langle \overrightarrow{u}, \overrightarrow{u} \rangle \langle \overrightarrow{v}, \overrightarrow{v} \rangle \leq 0.$$

Odtud dostáváme
$$\langle \overrightarrow{u}, \overrightarrow{v} \rangle^2 \leq \langle \overrightarrow{u}, \overrightarrow{u} \rangle \langle \overrightarrow{v}, \overrightarrow{v} \rangle,$$
a tedy
$$|\langle \overrightarrow{u}, \overrightarrow{v} \rangle| \leq \sqrt{\langle \overrightarrow{u}, \overrightarrow{u} \rangle}\sqrt{\langle \overrightarrow{v}, \overrightarrow{v} \rangle}.$$
Proto platí
$$|\langle \overrightarrow{u}, \overrightarrow{v} \rangle| \leq ||\overrightarrow{u}|| \cdot ||\overrightarrow{v}||.$$

d) Jsou-li $\overrightarrow{u}, \overrightarrow{v} \in E$, pak platí podle definice skalárního součinu a podle právě dokázaného vztahu c)
$$||\overrightarrow{u} + \overrightarrow{v}||^2 = \langle \overrightarrow{u} + \overrightarrow{v}, \overrightarrow{u} + \overrightarrow{v} \rangle = \langle \overrightarrow{u}, \overrightarrow{u} \rangle + 2\langle \overrightarrow{u}, \overrightarrow{v} \rangle + \langle \overrightarrow{v}, \overrightarrow{v} \rangle \leq$$
$$\leq ||\overrightarrow{u}||^2 + 2 \cdot ||\overrightarrow{u}|| \cdot ||\overrightarrow{v}|| + ||\overrightarrow{v}||^2 = (||\overrightarrow{u}|| + ||\overrightarrow{v}||)^2,$$
tzn.
$$||\overrightarrow{u} + \overrightarrow{v}|| \leq ||\overrightarrow{u}|| + ||\overrightarrow{v}||.$$

□

**Definice 10.3** Úhlem mezi vektory $\overrightarrow{u} \neq \overrightarrow{o}$, $\overrightarrow{v} \neq \overrightarrow{o}$ *eukleidovského vektorového prostoru* $\mathcal{E}$ *nazveme číslo*
$$\varphi = \arccos \frac{\langle \overrightarrow{u}, \overrightarrow{v} \rangle}{||\overrightarrow{u}|| \cdot ||\overrightarrow{v}||}.$$
*Platí tedy, že*
$$\cos\varphi = \frac{\langle \overrightarrow{u}, \overrightarrow{v} \rangle}{||\overrightarrow{u}|| \cdot ||\overrightarrow{v}||}, \text{ kde } 0 \leq \varphi \leq \pi.$$
*Jestliže* $\overrightarrow{u} = \overrightarrow{o}$ *nebo* $\overrightarrow{v} = \overrightarrow{o}$, *pak klademe* $\cos\varphi = 0$.

(Na základě Schwarzovy nerovnosti je zřejmé, že pojem úhlu mezi vektory je určen jednoznačně.)

**Definice 10.4** *Vektory* $\overrightarrow{u}$ *a* $\overrightarrow{v}$ *nazveme* ortogonální *(neboli* kolmé*) (značíme* $\overrightarrow{u} \perp \overrightarrow{v}$*), platí-li, že úhel* $\varphi$ *mezi vektory* $\overrightarrow{u}$ *a* $\overrightarrow{v}$ *je roven* $\frac{\pi}{2}$.

Tzn., že $\overrightarrow{u} \perp \overrightarrow{v}$ právě tehdy, když $\cos\varphi = 0$, a to platí tehdy a jen tehdy, když $\langle \overrightarrow{u}, \overrightarrow{v} \rangle = 0$.

**Věta 10.2** *Jsou-li* $\overrightarrow{u}, \overrightarrow{v_1}, \overrightarrow{v_2}, \ldots, \overrightarrow{v_m}$ *vektory eukleidovského prostoru* $\mathcal{E}$ *a platí-li* $\overrightarrow{u} \perp \overrightarrow{v_i}$ *pro každé* $i = 1, 2, \ldots, m$, *potom je vektor* $\overrightarrow{u}$ *ortogonální ke každému vektoru z podprostoru* $[\{\overrightarrow{v_1}, \overrightarrow{v_2}, \ldots, \overrightarrow{v_m}\}]$.

*(Budeme také říkat, že* $\overrightarrow{u}$ *je ortogonální k podprostoru* $[\{\overrightarrow{v_1}, \overrightarrow{v_2}, \ldots, \overrightarrow{v_m}\}]$.*)*

D ů k a z: Nechť $\overrightarrow{v} = [\{\overrightarrow{v_1}, \overrightarrow{v_2}, \ldots, \overrightarrow{v_m}\}]$, tj. existují čísla $c_1, c_2, \ldots, c_m \in \mathbb{R}$ tak, že

$$\overrightarrow{v} = \sum_{i=1}^{m} c_i \overrightarrow{v_i}.$$

Potom

$$\langle \overrightarrow{u}, \overrightarrow{v} \rangle = \left\langle \overrightarrow{u}, \sum_{i=1}^{m} c_i \overrightarrow{v_i} \right\rangle = \sum_{i=1}^{m} \langle \overrightarrow{u}, c_i \overrightarrow{v_i} \rangle =$$

$$= \sum_{i=1}^{m} c_i \langle \overrightarrow{u}, \overrightarrow{v_i} \rangle = \sum_{i=1}^{m} c_i \cdot 0 = 0,$$

tedy platí $\overrightarrow{u} \perp \overrightarrow{v_i}$. □

**Definice 10.5** *Jsou-li $\overrightarrow{u_1}, \overrightarrow{u_2}, \ldots, \overrightarrow{u_m}$ vektory eukleidovského vektorového prostoru $\mathcal{E}$, pak řekneme, že jsou (*vzájemně*) *ortogonální*, platí-li $\overrightarrow{u_i} \perp \overrightarrow{u_j}$ pro každé $i \neq j$, $i, j \in \{1, 2, \ldots, m\}$.*

**Věta 10.3** *Nenulové vzájemně ortogonální vektory $\overrightarrow{u_1}, \overrightarrow{u_2}, \ldots, \overrightarrow{u_m}$ jsou lineárně nezávislé.*

D ů k a z: Nechť $c_1, c_2, \ldots, c_m$ jsou taková čísla z $\mathbb{R}$, že

$$\sum_{i=1}^{m} c_i \overrightarrow{u_i} = \overrightarrow{o}.$$

Pro libovolné $k \in \{1, \ldots, m\}$ pak platí

$$0 = \langle \overrightarrow{o}, \overrightarrow{u_k} \rangle = \left\langle \sum_{i=1}^{m} c_i \overrightarrow{u_i}, \overrightarrow{u_k} \right\rangle = \sum_{i=1}^{m} c_i \langle \overrightarrow{u_i}, \overrightarrow{u_k} \rangle.$$

Protože $\overrightarrow{u_i} \perp \overrightarrow{u_k}$ pro každé $i \neq k$, platí

$$0 = \sum_{i=1}^{m} c_i \langle \overrightarrow{u_i}, \overrightarrow{u_k} \rangle = c_k \langle \overrightarrow{u_k}, \overrightarrow{u_k} \rangle.$$

Ovšem podle předpokladu $\overrightarrow{u_k} \neq \overrightarrow{o}$, tedy $\langle \overrightarrow{u_k}, \overrightarrow{u_k} \rangle > 0$, a proto $c_k = 0$. □

**Věta 10.4** *Jestliže množina nenulových vzájemně ortogonálních vektorů $\{\overrightarrow{u_1}, \ldots, \overrightarrow{u_n}\}$ generuje prostor $\mathcal{E}$, pak je bází prostoru $\mathcal{E}$.*

D ů k a z: Věta je bezprostředním důsledkem předchozí věty. □

## 10.2 Schmidtova ortogonalizační metoda

**Definice 10.6**

*a) Je-li báze* $M = \{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ *eukleidovského vektorového prostoru* $\mathcal{V}$ *složena z ortogonálních vektorů, pak* $M$ *se nazývá* ortogonální báze.

*b) Báze* $M = \{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ *se nazývá* ortonormální, *je-li ortogonální a platí-li pro každé* $i = 1, \dots, n$, *že* $||\overrightarrow{u_i}|| = 1$.

V další větě si ukážeme metodu, pomocí které budeme moci ortogonalizovat každou bázi eukleidovského vektorového prostoru.

**Věta 10.5 Schmidtova ortogonalizační metoda** *Je-li eukleidovský vektorový prostor* $\mathcal{E}$ *konečné dimenze, pak z každé konečné posloupnosti* $\overrightarrow{v_1}, \overrightarrow{v_2}, \dots, \overrightarrow{v_m}$ $(m \geq 1)$ *lineárně nezávislých vektorů prostoru* $\mathcal{E}$ *je možno vytvořit ortogonální posloupnost nenulových vektorů* $\overrightarrow{u_1}, \overrightarrow{u_2}, \dots, \overrightarrow{u_m}$, *kde*

$$\overrightarrow{u_i} = \overrightarrow{v_i} - \sum_{k=1}^{i-1} d_{ik}\overrightarrow{v_k}, i = 1, 2, \dots, m,$$

*pro kterou platí*

$$[\{\overrightarrow{u_1}, \overrightarrow{u_2}, \dots, \overrightarrow{u_m}\}] = [\{\overrightarrow{v_1}, \overrightarrow{v_2}, \dots, \overrightarrow{v_m}\}].$$

D ů k a z: Budeme dokazovat indukcí podle $m$.

Pro $m = 1$ je tvrzení triviální.

Předpokládejme, že $m > 1$ a že jsme již sestrojili posloupnost nenulových ortogonálních vektorů $\overrightarrow{u_1}, \dots, \overrightarrow{u_{m-1}}$, které jsou v žádaném tvaru a pro které platí

$$[\{\overrightarrow{u_1}, \dots, \overrightarrow{u_{m-1}}\}] = [\{\overrightarrow{v_1}, \dots, \overrightarrow{v_{m-1}}\}].$$

Položme

$$\overrightarrow{u_m} = \overrightarrow{v_m} - \sum_{k=1}^{m-1} c_{mk}\overrightarrow{u_k},$$

kde

$$c_{mk} = \frac{\langle \overrightarrow{v_m}, \overrightarrow{u_k} \rangle}{\langle \overrightarrow{u_k}, \overrightarrow{u_k} \rangle}.$$

Potom pro každé $j = 1, 2, \dots, m-1$ platí

$$\langle \overrightarrow{u_m}, \overrightarrow{u_j} \rangle = \langle \overrightarrow{v_m}, \overrightarrow{u_j} \rangle - \sum_{k=1}^{m-1} c_{mk}\langle \overrightarrow{u_k}, \overrightarrow{u_j} \rangle =$$

$$= \langle \overrightarrow{v_m}, \overrightarrow{u_j} \rangle - c_{mj}\langle \overrightarrow{u_j}, \overrightarrow{u_j} \rangle.$$

(Poslední rovnost jsme dostali ze skutečnosti, že podle předpokladu platí $\overrightarrow{u_k} \perp \overrightarrow{u_j}$ pro každé $k \in \{1, \dots, m-1\}$, $k \neq j$, a tedy $\langle \overrightarrow{u_k}, \overrightarrow{u_j} \rangle = 0$.)

Pro $c_{mj}$ platí (podle konstrukce $\overrightarrow{u_m}$), že

$$c_{mj}\langle\overrightarrow{u_j},\overrightarrow{u_j}\rangle = \langle\overrightarrow{v_m},\overrightarrow{u_j}\rangle,$$

tedy $\langle\overrightarrow{u_m},\overrightarrow{u_j}\rangle = 0$, tzn. $\overrightarrow{u_m}\perp\overrightarrow{u_j}$.

Vzhledem k tomu, že pro každé $k = 1,\dots,m-1$ platí

$$\overrightarrow{u_k} = \overrightarrow{v_k} - \sum_{j=1}^{k-1} d_{kj}\overrightarrow{v_j},$$

dostaneme

$$\overrightarrow{u_m} = \overrightarrow{v_m} - \sum_{k=1}^{m-1} c_{mk}\overrightarrow{u_k} = \overrightarrow{v_m} - \sum_{k=1}^{m-1} c_{mk}\left(\overrightarrow{v_k} - \sum_{j=1}^{k-1} d_{kj}\overrightarrow{v_j}\right) =$$

$$= \overrightarrow{v_m} - \sum_{k=1}^{m-1} c_{mk}\overrightarrow{v_k} + \sum_{k=1}^{m-1}\sum_{j=1}^{k-1} c_{mk}d_{kj}\overrightarrow{v_j} = \overrightarrow{v_m} - \sum_{k=1}^{m-1} d_{mk}\overrightarrow{v_k},$$

kde pro každé $k = 1,\dots,m-1$

$$d_{mk} = c_{mk} - \sum_{k<j<m} c_{mj}d_{jk}.$$

Tedy

$$\overrightarrow{u_m} = \overrightarrow{v_m} - \sum_{k=1}^{m-1} d_{mk}\overrightarrow{v_k},$$

tzn., že je vyjádřen v požadovaném tvaru. Navíc je zřejmé, že $\overrightarrow{u_m} \neq \overrightarrow{o}$, protože jinak by vektory $\overrightarrow{v_1},\dots,\overrightarrow{v_m}$ byly lineárně závislé.

Z předpokladu

$$[\{\overrightarrow{u_1},\dots,\overrightarrow{u_{m-1}}\}] = [\{\overrightarrow{v_1},\dots,\overrightarrow{v_{m-1}}\}]$$

a z toho, že $\overrightarrow{u_m} \in [\{\overrightarrow{v_1},\dots,\overrightarrow{v_m}\}]$, dostaneme

$$[\{\overrightarrow{u_1},\dots,\overrightarrow{u_{m-1}},\overrightarrow{u_m}\}] = [\{\overrightarrow{v_1},\dots,\overrightarrow{v_{m-1}},\overrightarrow{u_m}\}] \subseteq\subseteq [\{\overrightarrow{v_1},\dots,\overrightarrow{v_{m-1}},\overrightarrow{v_m}\}].$$

Analogicky dostaneme, že

$$[\{\overrightarrow{v_1},\dots,\overrightarrow{v_{m-1}},\overrightarrow{v_m}\}] \subseteq\subseteq [\{\overrightarrow{u_1},\dots,\overrightarrow{u_{m-1}},\overrightarrow{u_m}\}],$$

tedy vektory $\overrightarrow{u_1},\dots,\overrightarrow{u_m}$ a $\overrightarrow{v_1},\dots,\overrightarrow{v_m}$ generují stejné podprostory. $\square$

**Věta 10.6** *Každý nenulový podprostor eukleidovského vektorového prostoru $\mathcal{E}$ konečné dimenze má ortonormální bázi. Tedy speciálně: Každý nenulový eukleidovský vektorový prostor $\mathcal{E}$ konečné dimenze má ortonormální bázi.*

D ů k a z: Nechť $\mathcal{F}$ je podprostor prostoru $\mathcal{E}$, $\dim \mathcal{F} = m \geq 1$. Uvažujme libovolnou bázi $M = \{\overrightarrow{v_1}, \ldots, \overrightarrow{v_m}\}$ prostoru $\mathcal{F}$. Pak podle předchozí věty můžeme z $M$ vytvořit ortogonální bázi $M' = \{\overrightarrow{u_1}, \ldots, \overrightarrow{u_m}\}$ tohoto prostoru. Označme

$$\overrightarrow{z_i} = \frac{\overrightarrow{u_i}}{||\overrightarrow{u_i}||}$$

pro každé $i = 1, \ldots, m$. Platí, že $\{\overrightarrow{z_1}, \ldots, \overrightarrow{z_m}\}$ je také ortogonální bází prostoru $\mathcal{F}$ a že $||\overrightarrow{z_i}|| = 1$ pro každé $i = 1, \ldots, m$. $\square$

Shrneme ještě jednou postup, který umožňuje přejít od libovolné báze eukleidovského vektorového prostoru $\mathcal{E}$ konečné dimenze $n \geq 1$ k ortonormální bázi.

Nechť $\{\overrightarrow{v_1}, \ldots, \overrightarrow{v_n}\}$ je báze prostoru $\mathcal{E}$. Položme

$$\begin{aligned}
&\overrightarrow{u_1} = \overrightarrow{v_1},\\
&\overrightarrow{u_2} = \overrightarrow{v_2} - \tfrac{\langle \overrightarrow{v_2}, \overrightarrow{u_1}\rangle}{\langle \overrightarrow{u_1}, \overrightarrow{u_1}\rangle}\overrightarrow{u_1},\\
&\overrightarrow{u_3} = \overrightarrow{v_3} - \tfrac{\langle \overrightarrow{v_3}, \overrightarrow{u_2}\rangle}{\langle \overrightarrow{u_2}, \overrightarrow{u_2}\rangle}\overrightarrow{u_2} - \tfrac{\langle \overrightarrow{v_3}, \overrightarrow{u_1}\rangle}{\langle \overrightarrow{u_1}, \overrightarrow{u_1}\rangle}\overrightarrow{u_1},\\
&\vdots\\
&\overrightarrow{u_n} = \overrightarrow{v_n} - \tfrac{\langle \overrightarrow{v_n}, \overrightarrow{u_{n-1}}\rangle}{\langle \overrightarrow{u_{n-1}}, \overrightarrow{u_{n-1}}\rangle}\overrightarrow{u_{n-1}} - \cdots - \tfrac{\langle \overrightarrow{v_n}, \overrightarrow{u_1}\rangle}{\langle \overrightarrow{u_1}, \overrightarrow{u_1}\rangle}\overrightarrow{u_1}.
\end{aligned}$$

Potom $\{\overrightarrow{u_1}, \ldots, \overrightarrow{u_n}\}$ je ortogonální báze.

Abychom získali ortonormální bázi, stačí přejít od vektorů $\overrightarrow{u_1}, \ldots, \overrightarrow{u_n}$ k vektorům

$$\frac{\overrightarrow{u_1}}{||\overrightarrow{u_1}||}, \ldots, \frac{\overrightarrow{u_n}}{||\overrightarrow{u_n}||}.$$

**Příklad 10.3** Určete ortonormální bázi podprostoru v $\mathcal{R}^4$ uvažovaného s obyčejným skalárním součinem generovaného vektory $\overrightarrow{v_1}, \overrightarrow{v_2}, \overrightarrow{v_3}$, kde $\overrightarrow{v_1} = (1, 1, 0, 1)$, $\overrightarrow{v_2} = (1, -2, 0, 0)$, $\overrightarrow{v_3} = (1, 0, -1, 2)$.

Platí, že vektory $\overrightarrow{v_1}, \overrightarrow{v_2}, \overrightarrow{v_3}$ jsou lineárně nezávislé, tedy tvoří bázi prostoru $[\{\overrightarrow{v_1}, \overrightarrow{v_2}, \overrightarrow{v_3}\}]$. Na tuto bázi použijme Schmidtovu ortogonalizační metodu.

$$\begin{aligned}
&\overrightarrow{u_1} = \overrightarrow{v_1},\\
&\overrightarrow{u_2} = \overrightarrow{v_2} - \tfrac{\langle \overrightarrow{v_2}, \overrightarrow{u_1}\rangle}{\langle \overrightarrow{u_1}, \overrightarrow{u_1}\rangle}\overrightarrow{u_1} = (1, -2, 0, 0) - \tfrac{-1}{3}(1, 1, 0, 1) = (\tfrac{4}{3}, -\tfrac{5}{3}, 0, \tfrac{1}{3}) = \tfrac{1}{3}(4, -5, 0, 1)\\
&\overrightarrow{u_3} = \overrightarrow{v_3} - \tfrac{\langle \overrightarrow{v_3}, \overrightarrow{u_2}\rangle}{\langle \overrightarrow{u_2}, \overrightarrow{u_2}\rangle}\overrightarrow{u_2} - \tfrac{\langle \overrightarrow{v_3}, \overrightarrow{u_1}\rangle}{\langle \overrightarrow{u_1}, \overrightarrow{u_1}\rangle}\overrightarrow{u_1} = (1, 0, -1, 2) - \tfrac{2}{\frac{14}{3}}\tfrac{1}{3}(4, -5, 0, 1) - \tfrac{3}{3}(1, 1, 0, 1) =\\
&= (1, 0, -1, 2) - \tfrac{1}{7}(4, -5, 0, 1) - (1, 1, 0, 1) = (-\tfrac{4}{7}, -\tfrac{2}{7}, -1, \tfrac{6}{7}) = \tfrac{1}{7}(-4, -2, -7, 6).
\end{aligned}$$

Získané ortogonální vektory budeme normalizovat

$$\begin{aligned}
&\overrightarrow{z_1} = \tfrac{\overrightarrow{u_1}}{||\overrightarrow{u_1}||} = \tfrac{1}{\sqrt{3}}(1, 1, 0, 1),\\
&\overrightarrow{z_2} = \tfrac{\overrightarrow{u_2}}{||\overrightarrow{u_2}||} = \tfrac{\sqrt{3}}{\sqrt{14}}\tfrac{1}{3}(4, -5, 0, 1) = \tfrac{1}{\sqrt{42}}(4, -5, 0, 1),\\
&\overrightarrow{z_3} = \tfrac{\overrightarrow{u_3}}{||\overrightarrow{u_3}||} = \tfrac{7}{\sqrt{105}}\tfrac{1}{7}(-4, -2, -7, 6) = \tfrac{7}{\sqrt{105}}(-4, -2, -7, 6).
\end{aligned}$$

Platí, že $\{\overrightarrow{z_1}, \overrightarrow{z_2}, \overrightarrow{z_3}\}$ je hledaná ortonormální báze.

**Věta 10.7** *Jestliže $M = \{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ je ortonormální báze eukleidovského prostoru $\mathcal{E}$ a jsou-li*

$$\overrightarrow{u} = \sum_{i=1}^{n} c_i \overrightarrow{u_i}, \quad \overrightarrow{v} = \sum_{i=1}^{n} d_i \overrightarrow{u_i}$$

*libovolné vektory z $\mathcal{E}$ potom pro skalární součin vektorů $\overrightarrow{u}$ a $\overrightarrow{v}$ platí*

$$\langle \overrightarrow{u}, \overrightarrow{v} \rangle = \sum_{i=1}^{n} c_i d_i.$$

D ů k a z: Platí

$$\langle \overrightarrow{u}, \overrightarrow{v} \rangle = \left\langle \sum_{i=1}^{n} c_i \overrightarrow{u_i}, \sum_{i=1}^{n} d_i \overrightarrow{u_i} \right\rangle = \sum_{i,j=1}^{n} c_i d_j \langle \overrightarrow{u_i}, \overrightarrow{u_j} \rangle = \sum_{i=1}^{n} c_i d_i,$$

protože podle předpokladu $\langle \overrightarrow{u_i}, \overrightarrow{u_i} \rangle = 1$, $i = 1, \dots, n$, $\langle \overrightarrow{u_i}, \overrightarrow{u_j} \rangle = 0$, $i, j = 1, \dots, n$, $i \neq j$. $\square$

Při studiu vektorových prostorů (bez skalárního součinu) jsme dokázali, že všechny vektorové prostory konečné dimenze $n$ (nad stejným číselným tělesem $\mathcal{T}$) jsou navzájem izomorfní, tedy že mají stejné algebraické vlastnosti. Nyní zavedeme pojem izomorfizmu i pro eukleidovské vektorové prostory.

**Definice 10.7** *Eukleidovské vektorové prostory $(\mathcal{E}, g)$ a $(\mathcal{E}', g')$ se nazývají* izomorfní, *existuje-li takový izomorfizmus $\varphi$ vektorového prostoru $\mathcal{E}$ na vektorový prostor $\mathcal{E}'$, že*

$$\forall \overrightarrow{u}, \overrightarrow{v} \in E; g((\overrightarrow{u}, \overrightarrow{v})) = g'((\varphi(\overrightarrow{u}), \varphi(\overrightarrow{v}))).$$

*(Není-li nebezpečí nedorozumění, můžeme tuto podmínku také zapsat ve tvaru)*

$$\forall \overrightarrow{u}, \overrightarrow{v} \in E; \langle \overrightarrow{u}, \overrightarrow{v} \rangle = \langle \varphi(\overrightarrow{u}), \varphi(\overrightarrow{v}) \rangle.)$$

**Věta 10.8** *Každé dva eukleidovské vektorové prostory dimenze n jsou izomorfní.*

D ů k a z: Nechť $\{\overrightarrow{u_1}, \dots, \overrightarrow{u_n}\}$ je ortonormální báze prostoru $(\mathcal{E}, g)$, $\{\overrightarrow{u_1}', \dots, \overrightarrow{u_n}'\}$ ortonormální báze prostoru $(\mathcal{E}', g')$. Pak existuje právě jeden izomorfizmus $\varphi$ vektorového prostoru $\mathcal{E}$ na vektorový prostor $\mathcal{E}'$ takový, že $\overrightarrow{u_i}' = \varphi(\overrightarrow{u_i})$, $i = 1, \dots, n$. Ukážeme, že $\varphi$ je izomorfizmus eukleidovského prostoru $(\mathcal{E}, g)$ na eukleidovský prostor $(\mathcal{E}', g')$.

Nechť $\overrightarrow{u}, \overrightarrow{v} \in E$,

$$\overrightarrow{u} = \sum_{i=1}^{n} c_i \overrightarrow{u_i}, \overrightarrow{v} = \sum_{i=1}^{n} d_i \overrightarrow{u_i}.$$

Potom platí, že

$$\varphi(\overrightarrow{u}) = \sum_{i=1}^{n} c_i \overrightarrow{u_i}', \varphi(\overrightarrow{v}) = \sum_{i=1}^{n} d_i \overrightarrow{u_i}'.$$

Podle věty 10.7 pak dostáváme

$$g((\overrightarrow{u}, \overrightarrow{v})) = g'((\varphi(\overrightarrow{u}), \varphi(\overrightarrow{v}))) = \sum_{i=1}^{n} c_i d_i.$$

$\square$

## 10.3 Cvičení

**10.1** Určete některou ortogonální bázi podprostoru v $\mathcal{R}^4$ generovaného vektory $\overrightarrow{v_1} = (1, 1, -1, -2)$, $\overrightarrow{v_2} = (5, 8, -2, -3)$, $\overrightarrow{v_3} = (3, 9, 3, 8)$.
[ např. $\{\overrightarrow{v_1}, (2, 5, 1, 3)\}$ ]

**10.2** Určete ortonormální bázi podprostoru v $\mathcal{R}^4$ generovaného vektory $\overrightarrow{w_1} = (1, 2, 2, -1)$, $\overrightarrow{w_2} = (1, 1, -5, 3)$, $\overrightarrow{w_3} = (3, 2, 8, -7)$.
[ Např. $\{\sqrt{10}\overrightarrow{w_1}, \sqrt{26} \cdot (2, 3, -3, 2), \sqrt{10} \cdot (2, -1, -1, -2)\}$ ]

**10.3** Najděte některou ortogonální bázi vektorového prostoru řešení homogenní soustavy lineárních rovnic:

$$\begin{aligned} 3\xi_1 - \xi_2 - \xi_3 + \xi_4 &= 0 \\ \xi_1 + 2\xi_2 - \xi_3 - \xi_4 &= 0 \end{aligned}$$

[ např. {(1,-4,0,-7),(29,16,66,-5)} ]

# Kapitola 11

# Homomorfizmy vektorových prostorů konečné dimenze

V této kapitole budeme studovat vlastnosti homomorfizmů vektorových prostorů. Budeme si všímat zejména homomorfizmů prostorů, které mají konečnou dimenzi. V takovém případě existují úzké vztahy mezi homomorfizmy a maticemi, takže vlastnosti homomorfizmů budeme také popisovat pomocí vlastností matic.

## 11.1 Vlastnosti homomorfizmů

Připomeňme si, že jsou-li $\mathcal{V}$ a $\mathcal{V}'$ vektorové prostory nad číselným tělesem $\mathcal{T}$, pak zobrazení $f : V \to V'$ se nazývá *homomorfizmus* $\mathcal{V}$ do $\mathcal{V}'$, jestliže $f$ „přenáší" operaci sčítání vektorů a vnější operaci násobení vektorů skalárem, tj. $f(\overrightarrow{u} + \overrightarrow{v}) = f(\overrightarrow{u}) + f(\overrightarrow{v})$ a $f(c\overrightarrow{u}) = cf(\overrightarrow{u})$, pro každé $\overrightarrow{u}, \overrightarrow{v} \in V$ a $c \in T$. Obě podmínky lze také ekvivalentně nahradit jedinou podmínkou: $f(c\overrightarrow{u} + d\overrightarrow{v}) = cf(\overrightarrow{u}) + df(\overrightarrow{v})$, pro každé $\overrightarrow{u}, \overrightarrow{v} \in V$ a $c, d \in T$.

Jestliže homomorfizmus $f$ je zároveň bijektivním zobrazením $V$ na $V'$, pak $f$ se nazývá *izomorfizmus* $\mathcal{V}$ na $\mathcal{V}'$.

Místo názvu homomorfizmus vektorových prostorů se také používá název „*lineární zobrazení*".

Jestliže $\mathcal{V}$ na $\mathcal{V}'$ jsou libovolné vektorové prostory nad $\mathcal{T}$, pak zobrazení $o : V \longrightarrow V'$ takové, že $o(\overrightarrow{u}) = \overrightarrow{o}'$, kde $\overrightarrow{o}'$ je nulový vektor prostoru $\mathcal{V}'$, je homomorfizmus $\mathcal{V}$ do $\mathcal{V}'$.

Identické zobrazení $e_V : V \longrightarrow V$ je izomorfizmem $\mathcal{V}$ na $\mathcal{V}$.

**Věta 11.1** *Nechť $\mathcal{V}$ a $\mathcal{V}'$ jsou vektorové prostory nad $\mathcal{T}$ a $f$ je homomorfizmus $\mathcal{V}$ do $\mathcal{V}'$. Pak*

*a) Obraz* $\mathrm{Im} f$ *homomorfizmu $f$ je podprostorem prostoru $\mathcal{V}'$.*

*b) Jádro* $\mathrm{Ker} f$ *homomorfizmu $f$ je podprostorem prostoru $\mathcal{V}$.*

D ů k a z:

a) Nechť $\overrightarrow{x}, \overrightarrow{y} \in f(V) = \mathrm{Im}f$. Pak existují vektory $\overrightarrow{x}, \overrightarrow{y} \in V$ takové, že $f(\overrightarrow{u}) = \overrightarrow{x}, f(\overrightarrow{v}) = \overrightarrow{y}$. Tedy

$$\overrightarrow{x} + \overrightarrow{y} = f(\overrightarrow{u}) + f(\overrightarrow{v}) = f(\overrightarrow{u} + \overrightarrow{v}),$$

proto $\overrightarrow{x} + \overrightarrow{y} \in \mathrm{Im}f$. Podobně $c\overrightarrow{x} = c \cdot f(\overrightarrow{u}) = f(c\overrightarrow{u})$ a tedy také $c\overrightarrow{x} \in \mathrm{Im}f$.

b) Nechť $\overrightarrow{u}, \overrightarrow{v} \in \mathrm{Ker}f$. Pak $f(\overrightarrow{u}) = \overrightarrow{o}' = f(\overrightarrow{v})$, proto

$$f(\overrightarrow{u} + \overrightarrow{v}) = f(\overrightarrow{u}) + f(\overrightarrow{v}) = \overrightarrow{o}' + \overrightarrow{o}' = \overrightarrow{o}',$$

tedy $\overrightarrow{u} + \overrightarrow{v} \in \mathrm{Ker}f$. Podobně pro $c \in T$ a $\overrightarrow{u} \in \mathrm{Ker}f$ dostáváme

$$f(c\overrightarrow{u}) = cf(\overrightarrow{u}) = c \cdot \overrightarrow{o}' = \overrightarrow{o}',$$

proto $c\overrightarrow{u} \in \mathrm{Ker}f$.

□

Nechť nyní $\mathcal{V}$ je vektorový prostor konečné dimenze a $f$ je homomorfizmus $\mathcal{V}$ do $\mathcal{V}'$. Pak prostory $\mathrm{Ker}f$ a $\mathrm{Im}f$ mají také konečnou dimenzi.

**Definice 11.1** *Jestliže $f$ je homomorfizmus $\mathcal{V}$ do $\mathcal{V}'$ a $\mathcal{V}$ má konečnou dimenzi, pak* $\dim \mathrm{Ker}f$ *se nazývá* defekt homomorfizmu a $\dim \mathrm{Im}f$ *se nazývá* hodnost homomorfizmu $f$.

**Věta 11.2** *Jestliže $f$ je homomorfizmus vektorového prostoru $\mathcal{V}$ do vektorového prostoru $\mathcal{V}'$ a jestliže* $\dim \mathcal{V} = n$, *pak*

$$\dim \mathrm{Ker}f + \dim \mathrm{Im}f = n.$$

D ů k a z: Nechť $\dim \mathrm{Ker}f = r$, nechť $\{\overrightarrow{e_1}, \ldots, \overrightarrow{e_r}\}$ je báze prostoru $\mathrm{Ker}f$ a nechť $\{\overrightarrow{e_1}, \ldots, \overrightarrow{e_r}, \overrightarrow{e_{r+1}}, \ldots, \overrightarrow{e_n}\}$ je báze prostoru $\mathcal{V}$. Ukážeme, že množina $\{f(\overrightarrow{e_{r+1}}), \ldots, f(\overrightarrow{e_n})\}$ je bází prostoru $\mathrm{Im}f$.

Nechť $c_{r+1}f(\overrightarrow{e_{r+1}}) + \ldots + c_nf(\overrightarrow{e_n}) = \overrightarrow{o}'$. Pak $f(c_{r+1}\overrightarrow{e_{r+1}} + \ldots + c_n\overrightarrow{e_n}) = \overrightarrow{o}'$, tedy podle definice jádra platí $c_{r+1}\overrightarrow{e_{r+1}} + \ldots + c_n\overrightarrow{e_n} \in \mathrm{Ker}f$. Proto existují $c_1, \ldots, c_r \in T$ takové, že

$$c_1\overrightarrow{e_1} + \ldots + c_r\overrightarrow{e_r} = c_{r+1}\overrightarrow{e_{r+1}} + \ldots + c_n\overrightarrow{e_n},$$

neboli

$$c_1\overrightarrow{e_1} + \ldots + c_r\overrightarrow{e_r} - c_{r+1}\overrightarrow{e_{r+1}} - \ldots - c_n\overrightarrow{e_n} = \overrightarrow{o}'.$$

Protože $\{e_1, \ldots, e_n\}$ je báze prostoru $\mathcal{V}$, musí platit $c_1 = \ldots = c_n = 0$, tedy vektory $f(\overrightarrow{e_{r+1}}), \ldots, f(\overrightarrow{e_n})$ jsou lineárně nezávislé.

Nechť nyní $\overrightarrow{v} \in \mathrm{Im}f$. Pak existuje vektor $\overrightarrow{u} \in \mathcal{V}$ takový, že $f(\overrightarrow{u}) = \overrightarrow{v}$. Nechť $\overrightarrow{u} = \sum_{i=1}^{n} d_i\overrightarrow{e_i}$, kde $d_1, \ldots, d_n \in T$. Pak

$$\overrightarrow{v} = f(\overrightarrow{u}) = d_1f(\overrightarrow{e_1}) + \ldots + d_rf(\overrightarrow{e_r}) + d_{r+1}f(\overrightarrow{e_{r+1}}) + \ldots + d_nf(\overrightarrow{e_n}).$$

Přitom podle předpokladu $\overrightarrow{e_1}, \ldots, \overrightarrow{e_r} \in \mathrm{Ker} f$, proto $f(\overrightarrow{e_1}) = \ldots = f(\overrightarrow{e_r}) = \overrightarrow{o}'$, a tedy $\overrightarrow{v} = d_{r+1} f(\overrightarrow{e_{r+1}}) + \ldots + d_n f(e_n)$. To znamená, že $\overrightarrow{v} \in [\{f(\overrightarrow{e_{r+1}}), \ldots, f(\overrightarrow{e_n})\}]$, a protože $\overrightarrow{v}$ je libovolný vektor z $\mathrm{Im} f$, dostáváme, že $[\{f(\overrightarrow{e_{r+1}}), \ldots, f(\overrightarrow{e_n})\}] = \mathrm{Im} f$, neboli, že $\{f(\overrightarrow{e_{r+1}}), \ldots, f(\overrightarrow{e_n})\}$ je množina generátorů prostoru $\mathrm{Im} f$. Proto je také jeho bází.

Odtud vyplývá, že $\dim \mathrm{Im} f = n - r = n - \mathrm{Ker} f$. □

Následující věta je bezprostředním důsledkem.

**Věta 11.3** *Nechť $f$ je homomorfizmus $\mathcal{V}$ do $\mathcal{V}'$ a nechť $\mathcal{V}$ má konečnou dimenzi. Pak $f$ je injektivní, právě když je splněna některá z následujících podmínek.*

1. $\mathrm{Ker} f = \{\overrightarrow{o}\}$.
2. $\dim \mathrm{Im} f = \dim \mathcal{V}$.

Připomeňme, že složením dvou homomorfizmů vektorových prostorů získáme opět homomorfizmus. Nyní zavedeme dvě další operace s homomorfizmy.

**Definice 11.2**

a) *Nechť $f$ a $g$ jsou homomorfizmy vektorového prostoru $\mathcal{V}$ do vektorového prostoru $\mathcal{V}'$. Pak* součtem *homomorfizmů $f$ a $g$ rozumíme zobrazení $f + g : V \longrightarrow V'$ takové, že pro každý $\overrightarrow{x} \in V$*

$$(f+g)(\overrightarrow{x}) = f(\overrightarrow{x}) + g(\overrightarrow{x}).$$

b) *Jestliže $f$ je homomorfizmus $\mathcal{V}$ do $\mathcal{V}'$ a $c \in T$, pak* $c$-násobkem *(*skalárním násobkem*) homomorfizmu $f$ nazýváme zobrazení $cf : V \longrightarrow V'$ takové, že pro každý $\overrightarrow{x} \in V$*

$$(cf)(\overrightarrow{x}) = c \cdot f(\overrightarrow{x}).$$

**Věta 11.4** *Součet, skalární násobek a složení homomorfizmů jsou homomorfizmy vektorových prostorů.*

Všude v dalším budeme uvažovat vektorové prostory nad tělesem $\mathcal{T}$. Jestliže $\mathcal{V}$ je vektorový prostor a je konečné dimenze $n$, pak k jeho označení budeme také používat symbolu $\mathcal{V}_n$.

Nechť $\mathcal{V}_n$ a $\mathcal{W}_m$ jsou vektorové prostory. Označme $\mathrm{Hom}(\mathcal{V}_n, \mathcal{W}_m)$ množinu všech homomorfizmů prostoru $\mathcal{V}_n$ do prostoru $\mathcal{W}_m$.

**Věta 11.5** *Pro libovolné vektorové prostory $\mathcal{V}_n$ a $\mathcal{W}_n$ nad $\mathcal{T}$ je $(\mathrm{Hom}(\mathcal{V}_n, \mathcal{W}_m), +, \mathcal{T}, \cdot)$, kde $+$ je sčítání homomorfizmů a $\cdot$ je levá vnější operace skalárního násobku homomorfizmů, vektorovým prostorem nad $\mathcal{T}$. Přitom platí, že $\dim \mathrm{Hom}(\mathcal{V}_n, \mathcal{W}_m) = n \cdot m$.*

D ů k a z: Vždy existuje alespoň nulový homomorfizmus $o : V_n \longrightarrow W_m$, proto $\mathrm{Hom}(\mathcal{V}_n, \mathcal{W}_m) \neq 0$.

1. Podle věty 11.4 je $(\mathrm{Hom}(\mathcal{V}_n, \mathcal{W}_m), +)$ grupoid. Komutativnost a asociativnost sčítání vyplývá přímo z definice. Homomorfizmus $o$ je nulovým prvkem a jestliže $f : V_n \longrightarrow W_m$ je homomorfizmus, pak jeho opačným prvkem je zobrazení $-f : V_n \longrightarrow W_m$ takové, že $(-f)(\overrightarrow{x}) = -f(\overrightarrow{x})$ pro každý vektor $\overrightarrow{x} \in V_n$.

   Tedy $(\mathrm{Hom}(\mathcal{V}_n, \mathcal{W}_m), +)$ je abelovská grupa.

2. Nechť např. $c, d \in T$ a $f, g \in \mathrm{Hom}(\mathcal{V}_n, \mathcal{W}_m)$. Jestliže $\overrightarrow{x} \in V_n$, pak $((c+d)f)(\overrightarrow{x}) = (c+d)f(\overrightarrow{x}) = cf(\overrightarrow{x}) + df(\overrightarrow{x}) = (cf)(\overrightarrow{x}) + (df)(\overrightarrow{x})$. Tedy platí $(c+d)f = cf + df$. Podobně se ověří zbývající axiómy pro násobení vektorů skalárem z definice vektorového prostoru.

3. Nyní dokážeme tvrzení o dimenzi vektorového prostoru homomorfizmů.

   Nechť $\{\overrightarrow{e_1}, \ldots, \overrightarrow{e_n}\}$ je báze prostoru $\mathcal{V}_n$ a $\{\overrightarrow{a_1}, \ldots, \overrightarrow{a_m}\}$ je báze prostoru $\mathcal{W}_m$. Definujme zobrazení $\varphi_{ji} : V_n \longrightarrow W_m$ $(i = 1, \ldots, m, j = 1, \ldots, n)$ takové, že je-li $\overrightarrow{x} \in V_n$ a $\overrightarrow{x} = x_1\overrightarrow{e_1} + \ldots + x_n\overrightarrow{e_n}$, pak $\varphi_{ji}(\overrightarrow{x}) = x_j\overrightarrow{a_i}$. Dostáváme tak $n \cdot m$ homomorfizmů prostoru $\mathcal{V}_n$ a $\mathcal{W}_m$. Dokážeme, že $\{\varphi_{ji}; i = 1, \ldots, m, j = 1, \ldots, n\}$ je bází prostoru $\mathrm{Hom}(\mathcal{V}_n, \mathcal{W}_m)$.

   a) Nejdříve ukážeme, že vektory $\varphi_{ji}$ jsou lineárně nezávislé. Nechť
   $$\sum_{j=1}^{n}\sum_{i=1}^{m} a_{ji}\varphi_{ji} = o$$
   pro některá $a_{ji} \in T$. Tzn., že
   $$\sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij}\varphi_{ji}(\overrightarrow{x}) = \overrightarrow{o}$$
   pro každý vektor $\overrightarrow{x} \in V_n$.
   Nechť $\overrightarrow{x} = \overrightarrow{e_1}$. Pak pro libovolné $i = 1, \ldots, m$ platí $\varphi_{ji}(\overrightarrow{e_1}) = 0 \cdot \overrightarrow{a_i} = \overrightarrow{o}$, jestliže $j \neq 1$, a $\varphi_{1i}(\overrightarrow{e_1}) = 1 \cdot \overrightarrow{a_i} = \overrightarrow{a_i}$. Tedy
   $$\sum_{j=1}^{n}\sum_{i=1}^{m} \overrightarrow{a_{ji}}\varphi_{ji}(\overrightarrow{e_1}) = a_{11}\varphi_{11}(\overrightarrow{e_1}) + \ldots + a_{1m}\varphi_{1m}(\overrightarrow{e_m}) = a_{11}\overrightarrow{a_1} + \ldots + a_{1m}\overrightarrow{a_m} = \overrightarrow{o}.$$
   Přitom vektory $\overrightarrow{a_1}, \ldots, \overrightarrow{a_m}$ jsou podle předpokladu lineárně nezávislé, proto $a_{11} = \ldots = a_{1m} = 0$. Podobně pro $\overrightarrow{x} = \overrightarrow{e_j}$ $(j = 2, \ldots, n)$ dostaneme $a_{j1} = \ldots = a_{jm} = 0$, a tedy vektory $\varphi_{ji}$, $i = 1, \ldots, m, j = 1, \ldots, n$ tvoří lineárně nezávislou množinu.

   b) Zbývá dokázat, že tato množina také generuje prostor $\mathrm{Hom}(\mathcal{V}_n, \mathcal{W}_m)$. Nechť $f : V_n \longrightarrow W_m$ je libovolný homomorfizmus a $\overrightarrow{x} = x_1\overrightarrow{e_1} + \ldots + x_n\overrightarrow{e_n} \in V_n$. Pak $f(\overrightarrow{x}) = x_1f(e_1) + \ldots x_nf(\overrightarrow{e_n})$. Protože $f(\overrightarrow{e_1}), \ldots, f(\overrightarrow{e_n}) \in \mathcal{W}_m$, existují $a_{ji} \in T$

$(i = 1, \ldots, n, j = 1, \ldots, m)$ taková, že

$$\begin{aligned} f(\overrightarrow{e_1}) &= a_{11}\overrightarrow{a_1} + \ldots + a_{1m}\overrightarrow{a_m}, \\ &\vdots \\ f(\overrightarrow{e_n}) &= a_{n1}\overrightarrow{a_1} + \ldots + a_{nm}\overrightarrow{a_m}, \end{aligned}$$

a proto

$$\left(\sum_{j=1}^{n}\sum_{i=1}^{m} a_{ji}\varphi_{ji}\right)(\overrightarrow{x}) = \sum_{j=1}^{n}\sum_{i=1}^{m} a_{ji}\varphi_{ji}(\overrightarrow{x}) =$$

$$\sum_{j=1}^{n}\sum_{i=1}^{m} a_{ji}x_j\overrightarrow{a_i} = \sum_{j=1}^{n} x_j \sum_{i=1}^{m} a_{ji}\overrightarrow{a_i} = f(\overrightarrow{x}).$$

Tedy $f = \sum\limits_{j=1}^{n}\sum\limits_{i=1}^{m} a_{ji}\varphi_{ji}$. Protože $f$ byl libovolný homomorfizmus (tj. vektor) z $\mathrm{Hom}(\mathcal{V}_n, \mathcal{W}_m)$, dostáváme, že

$$[\{\varphi_{ji}, i = 1, \ldots, n, j = 1, \ldots, m\}] = \mathrm{Hom}(\mathcal{V}_n, \mathcal{W}_m).$$

$\square$

## 11.2 Matice homomorfizmů

**Věta 11.6** *Jestliže $\mathcal{V} = \mathcal{V}_n$ a $\mathcal{W}$ jsou vektorové prostory nad $\mathcal{T}$, pak každý homomorfizmus prostoru $\mathcal{V}$ do prostoru $\mathcal{W}$ je jednoznačně určen obrazy libovolné báze prostoru $\mathcal{V}$.*

D ů k a z: Nechť $\{\overrightarrow{e_1}, \ldots, \overrightarrow{e_n}\}$ je báze ve $\mathcal{V}$ a $f$ je homomorfizmus $\mathcal{V}$ do $\mathcal{W}$. Jestliže $\overrightarrow{x} = \sum\limits_{i=1}^{n} x_i\overrightarrow{e_i}$ je libovolný vektor z $V$, pak $\varphi(\overrightarrow{x}) = \sum\limits_{i=1}^{n} x_i f(\overrightarrow{e_i})$, tedy množina $\{f(\overrightarrow{e_1}), \ldots, f(\overrightarrow{e_n})\}$ jednoznačně určuje zobrazení $f$. $\square$

Jako důsledek dostáváme následující tvrzení

**Věta 11.7** *Jestliže $\overrightarrow{b_1}, \ldots, \overrightarrow{b_n}$ jsou libovolné vektory z $W$ a $\{\overrightarrow{e_1}, \ldots, \overrightarrow{e_n}\}$ je báze ve $\mathcal{V}$, pak existuje jediný homomorfizmus $f$ prostoru $\mathcal{V}$ do prostoru $\mathcal{W}$ takový, že $f(\overrightarrow{e_i}) = \overrightarrow{b_i}$, $i = 1, \ldots, n$.*

Všude v dalším se budeme věnovat homomorfizmům, které zobrazují daný vektorový prostor $\mathcal{V}$ opět do $\mathcal{V}$.

**Definice 11.3** Endomorfizmem *(nebo také* lineární transformací*) vektorového prostoru $\mathcal{V}$ rozumíme libovolný homomorfizmus prostoru $\mathcal{V}$ do $\mathcal{V}$.*

Ukážeme si nyní, jak je možné k zadání endomorfizmů vektorových prostorů a k práci s nimi využít matic. Nebude-li poznamenáno něco jiného, $\mathcal{V}$ bude vždy označovat vektorový prostor dimenze $n$.

**Definice 11.4** *Nechť $f$ je endomorfizmus vektorového prostoru $\mathcal{V}$. Jestliže je $M = \{\overrightarrow{e_1}, \dots, \overrightarrow{e_n}\}$ báze ve $\mathcal{V}$ a jestliže*

$$f(\overrightarrow{e_1}) = \sum_{i=1}^{n} a_{1i}\overrightarrow{e_i}, \dots, f(\overrightarrow{e_n}) = \sum_{i=1}^{n} a_{ni}\overrightarrow{e_i},$$

*pak matice $A = ||a_{ij}||$ se nazývá* matice endomorfizmu $f$ vzhledem k bázi $M$.

**Věta 11.8** *Existuje vzájemně jednoznačná korespondence mezi všemi endomorfizmy vektorového prostoru $\mathcal{V}$ a všemi čtvercovými maticemi z $M_n(\mathcal{T})$.*

D ů k a z: Zvolme některou bázi $M = \{\overrightarrow{e_1}, \dots, \overrightarrow{e_n}\}$ ve $\mathcal{V}$. Libovolnému endomorfizmu prostoru $\mathcal{V}$ přiřadíme jeho matici vzhledem k $M$.

Obráceně, nechť $A = ||a_{ij}|| \in M_n(\mathcal{T})$. Pak pro vektory $\overrightarrow{b_i} = \sum\limits_{j=1}^{n} a_{ij}\overrightarrow{e_j}$, $i = 1, \dots, n$, existuje podle věty 11.7 jediný endomorfizmus $f$ na $\mathcal{V}$ takový, že $f(\overrightarrow{e_i}) = \overrightarrow{b_i}$. Z vyjádření vektorů $\overrightarrow{b_1}, \dots, \overrightarrow{b_n}$ ve tvaru lineárních kombinací vektorů báze $M$ je vidět, že maticí endomorfizmu $f$ vzhledem k $M$ je právě matice $A$. □

**Věta 11.9** *Nechť $M = \{\overrightarrow{e_1}, \dots, \overrightarrow{e_n}\}$ je báze ve $\mathcal{V}$ a nechť $f$ je endomorfizmus prostoru $\mathcal{V}$, který má matici $A = ||a_{ij}||$ vzhledem k $M$. Pak pro každý vektor $\overrightarrow{x} \in V$ platí*

$$\{f(\overrightarrow{x})\}_M = \{\overrightarrow{x}\}_M \cdot A.$$

D ů k a z: Nechť $\{\overrightarrow{x}\}_M = (x_1, \dots, x_n)$, tzn. $\overrightarrow{x} = \sum\limits_{i=1}^{n} x_i\overrightarrow{e_i}$. Pak

$$f(\overrightarrow{x}) = \sum_{i=1}^{n} x_i f(\overrightarrow{e_i}) = \sum_{i=1}^{n} x_i \sum_{j=1}^{n} a_{ij}\overrightarrow{e_j} = \sum_{j=1}^{n} \left( \sum_{i=1}^{n} x_i a_{ij} \right) \overrightarrow{e_j},$$

a tedy

$$\{f(\overrightarrow{x})\}_M = \left( \sum_{i=1}^{n} x_i a_{i1}, \dots, \sum_{i=1}^{n} x_i a_{in} \right) = \{\overrightarrow{x}\}_M \cdot A.$$

□

**Definice 11.5** *Jestliže $A, B \in M_n(\mathcal{T})$, pak $A$ a $B$ se nazývají* podobné matice, *existuje-li regulární matice $Q \in M_n(\mathcal{T})$ taková, že $A = QBQ^{-1}$.*

**Věta 11.10** *Jestliže $f$ je endomorfizmus vektorového prostoru $\mathcal{V}$ a $M$ a $M'$ jsou báze ve $\mathcal{V}$, pak matice endomorfizmu $f$ vzhledem k bázím $M$ a $M'$ jsou podobné.*

D ů k a z: Nechť $M$ a $M'$ jsou báze ve $\mathcal{V}$, nechť $T$ je matice přechodu od báze $M$ k bázi $M'$ a nechť $A$, resp. $A'$, je matice endomorfizmu $f$ vzhledem k $M$, resp. $M'$. Podle předchozí věty platí pro každý $\overrightarrow{x} \in V$

$$\{f(\overrightarrow{x})\}_M = \{\overrightarrow{x}\}_M \cdot A, \{f(\overrightarrow{x})\}_{M'} = \{\overrightarrow{x}\}_{M'} \cdot A'.$$

Dále podle věty o transformacích souřadnic dostáváme

$$\{\overrightarrow{x}\}_M = \{\overrightarrow{x}\}_M \cdot T, \{f(\overrightarrow{x})\}_M = \{f(\overrightarrow{x})\}_{M'} \cdot T.$$

Proto

$$\{\overrightarrow{x}\}_M \cdot A = \{\overrightarrow{x}\}_{M'} \cdot T \cdot A.$$

a také

$$\{\overrightarrow{x}\}_M \cdot A = \{f(\overrightarrow{x})\}_M = \{f(\overrightarrow{x})\}_{M'} \cdot T = \{\overrightarrow{x}\}_{M'} \cdot A' \cdot T.$$

Pro libovolný vektor $\overrightarrow{x} \in V$ tak dostáváme, že $\{\overrightarrow{x}\}_{M'} \cdot T \cdot A = \{\overrightarrow{x}\}_{M'} \cdot A' \cdot T$, proto platí $TA = A'T$. Matice $T$ je jako matice přechodu regulární, takže dostáváme

$$A' = TAT^{-1}.$$

□

`Poznámka`: Maticová rovnost odvozená v důkazu současně dává návod, jak určit matici $f$ vzhledem k $M'$, známe-li matici $f$ vzhledem k $M$ a matici přechodu od $M$ k $M'$.

**Věta 11.11** *Nechť $f$ a $g$ jsou endomorfizmy vektorového prostoru $\mathcal{V}$ s maticemi $A$ a $B$ vzhledem k bázi $M$. Pak endomorfizmy $f \circ g, f+g$ a $cf (c \in T)$ mají vzhledem k $M$ postupně matice $AB$, $A+B$ a $cA$.*

D ů k a z: Nechť $\overrightarrow{x} \in V$. Pak platí:

a) $\{(f \circ g)(\overrightarrow{x})\}_M = \{g(f(\overrightarrow{x}))\}_M = \{f(\overrightarrow{x})\}_M \cdot B = \{\overrightarrow{x}\}_M \cdot AB$.

b) $\{(f+g)(\overrightarrow{x})\}_M = \{f(\overrightarrow{x})+g(\overrightarrow{x})\}_M = \{f(\overrightarrow{x})\}_M+\{g(\overrightarrow{x})\}_M = \{\overrightarrow{x}\}_M \cdot A+\{\overrightarrow{x}\}_M \cdot B = \{\overrightarrow{x}\}_M(A+B)$.

c) Analogicky dokážeme, že $\{(cf)(\overrightarrow{x})\}_M = \{\overrightarrow{x}\}_M \cdot cA$.

□

**Věta 11.12** *Nechť $f$ je endomorfizmus ve $\mathcal{V}$ a nechť $A$ je jeho matice vzhledem k některé bázi prostoru $\mathcal{V}$. Pak hodnost matice $A$ je rovna hodnosti endomorfizmu $f$.*

D ů k a z: Nechť $M = \{\overrightarrow{e_1}, \ldots, \overrightarrow{e_n}\}$ je báze ve $\mathcal{V}$ a nechť $A = ||a_{ij}||$. Pak

$$f(\overrightarrow{e_1}) = \sum_{j=1}^{n} a_{1j}\overrightarrow{e_j}, \ldots, f(\overrightarrow{e_n}) = \sum_{j=1}^{n} a_{nj}\overrightarrow{e_j}.$$

Protože vektory $f(\overrightarrow{e_1}), \ldots, f(\overrightarrow{e_n})$ generují prostor Im$f$, je jeho dimenze (tj. hodnost $f$) rovna maximálnímu počtu lineárně nezávislých vektorů mezi vektory $f(\overrightarrow{e_1}), \ldots, f(\overrightarrow{e_n})$. Přitom řádky matice $A$ jsou tvořeny právě souřadnicemi těchto vektorů vzhledem k $M$, a proto $h(A) = \dim \mathrm{Im} f$. □

## 11.3 Charakteristické kořeny, vlastní čísla a vlastní vektory endomorfizmů

**Definice 11.6** *Nechť $A = ||a_{ij}|| \in M_n(\mathcal{T})$. Pak matice $A - \lambda E \in M_n(\mathcal{T})$, kde $\lambda$ je parametr, se nazývá* charakteristická matice k matici *$A$.*

`Poznámka`: Matice $A - \lambda E$ je tedy ve tvaru

$$A - \lambda E = \begin{pmatrix} a_{11} - \lambda & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} - \lambda & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} - \lambda \end{pmatrix},$$

proto její determinant je polynomem v proměnné $\lambda$, který má stupeň $n$. Jeho koeficient u $\lambda^n$ je $(-1)^n\lambda^n$, koeficient u $\lambda^{(n-1)}$ je $(-1)^{(n-1)}(a_{11} + \ldots + a_{nn})$ a absolutní člen je roven det$A$.

**Definice 11.7** *Polynom* $\det(A - \lambda E)$ *se nazývá* charakteristický polynom *matice $A$ a jeho kořeny se nazývají* charakteristické kořeny *matice $A$.*

**Věta 11.13** *Jestliže $A$ a $B$ jsou podobné matice, pak $A$ a $B$ mají stejný charakteristický polynom (a tedy i stejné charakteristické kořeny).*

D ů k a z: Nechť $B = QAQ^{-1}$. Pak $\det(QAQ^{-1} - \lambda E) = \det(QAQ^{-1} - Q\lambda EQ^{-1}) = \det Q \cdot \det(A - \lambda E) \cdot \det Q^{-1} = \det Q \cdot \det(A - \lambda E) \cdot (\det Q)^{-1} = \det(A - \lambda E)$. □

**Definice 11.8** *Nechť $f$ je endomorfizmus vektorového prostoru $\mathcal{V}$ a nechť $A$ je jeho matice vzhledem k některé bázi. Pak charakteristickými kořeny endomorfizmu $f$ budeme rozumět charakteristické kořeny matice $A$.*

`Poznámka`: Podle vět 11.10 a 11.13 nezáleží v definici 11.8 na tom, vzhledem ke které bázi známe matici endomorfizmu $f$.

**Definice 11.9** *Nechť $f$ je endomorfizmus vektorového prostoru $\mathcal{V}$ a $A$ je jeho matice vzhledem k některé bázi. Nechť $\overrightarrow{o} \neq \overrightarrow{b} \in V$ a $\lambda_0 \in T$. Jestliže $\overrightarrow{b}A = \lambda_0 \overrightarrow{b}$, pak $\overrightarrow{b}$ se nazývá* vlastní vektor *a $\lambda_0$ se nazývá* vlastní číslo *endomorfizmu $f$ (a také* vlastní vektor *a* vlastní číslo *matice $A$). Říkáme pak, že vlastní vektor $\overrightarrow{b}$ přísluší k vlastnímu číslu $\lambda_0$.*

`Poznámka`: Protože $\overrightarrow{b} \neq \overrightarrow{o}$, je číslo $\lambda_0$ vektorem $\overrightarrow{b}$ určeno jednoznačně.

**Věta 11.14** *Vlastními čísly endomorfizmu $f$ jsou právě všechny charakteristické kořeny endomorfizmu $f$.*

D ů k a z: Nechť $M = \{\overrightarrow{e_1}, \dots, \overrightarrow{e_n}\}$ je báze prostoru $\mathcal{V}$ a nechť $A = ||a_{ij}||$ je matice endomorfizmu $f$ vzhledem k $M$. Předpokládejme, že $\overrightarrow{o} \neq \overrightarrow{b} \in V, \lambda_0 \in T$, a že $\overrightarrow{b}A = \lambda_0 \overrightarrow{b}$. Pak $\overrightarrow{b}(A - \lambda_0 E) = \overrightarrow{o}$, proto homogenní soustava $\xi(A - \lambda_0 E) = \overrightarrow{o}$ má netriviální řešení $\overrightarrow{b}$, a to znamená, že $\lambda_0$ je charakteristický kořen endomorfizmu $f$. (V předcházejících kapitolách jsme pro soustavy lineárních rovnic používali maticový zápis ve tvaru $B\overrightarrow{\xi}^T = \overrightarrow{c}^T$. Pokud bychom chtěli použít i zde takový zápis, museli bychom přejít k transponovaným maticím, tj. soustavu $\overrightarrow{\xi}(A - \lambda_0 E) = \overrightarrow{o}$ bychom zapsali ve tvaru $(A^T - \lambda_0 E)\overrightarrow{\xi}^T = \overrightarrow{o}^T$. Stejně i v dalším textu.)

Obráceně, nechť $\lambda_0$ je charakteristický kořen $f$, tedy také charakteristický kořen matice $A$. Proto $\det(A - \lambda_0 E) = 0$, neboli matice $A - \lambda_0 E$ je singulární, a tedy homogenní soustava $\overrightarrow{\xi}(A - \lambda_0 E)$ má nenulové řešení. Nechť $\overrightarrow{b} \neq \overrightarrow{o}$ je takové řešení. Pak $\overrightarrow{b}(A - \lambda_0 E) = \overrightarrow{o}$, neboli $\overrightarrow{b}A - \lambda_0 \overrightarrow{b}E = \overrightarrow{o}$, a odtud dostáváme $\overrightarrow{b}A = \lambda_0 \overrightarrow{b}$. Proto $\lambda_0$ je vlastním číslem endomorfizmu $f$. □

`Poznámka`: Právě dokázaná věta také říká, že v definici vlastních vektorů a vlastních čísel endomorfizmu $f$ nebyl podstatný výběr báze ve $\mathcal{V}$.

**Věta 11.15** *Množina všech vlastních vektorů matice $A$ (popř. endomorfizmu $f$), které jsou příslušné k vlastnímu číslu $\lambda_0$, spolu s nulovým vektorem, je podprostorem $\mathcal{W}_{\lambda_0}$ prostoru $\mathcal{V}$. Jeho dimenze je $n - h(A - \lambda_0 E)$.*

D ů k a z: Při dokazování věty 11.14 jsme zjistili, že vlastní vektory matice $A$ jsou právě nenulová řešení homogenní soustavy $(A^T - \lambda_0 E)\overrightarrow{\xi}^T = \overrightarrow{o}^T$. Přitom z teorie o homogenních soustavách lineárních rovnic je známo, že pro libovolnou homogenní soustavu $B\overrightarrow{\xi}^T = \overrightarrow{o}^T$ platí, že její řešení tvoří vektorový prostor, který má dimenzi $n - h(B)$. □

**Věta 11.16** *Jestliže $f$ je endomorfizmus vektorového prostoru $\mathcal{V}$ a $\lambda_0 \in T$, pak $\lambda_0$ je vlastním číslem endomorfizmu $f$ právě tehdy, když $f(\overrightarrow{b}) = \lambda_0 \overrightarrow{b}$ pro některý $\overrightarrow{o} \neq \overrightarrow{b} \in V$. Vlastními vektory endomorfizmu $f$ příslušnými k $\lambda_0$ jsou právě všechny vektory $\overrightarrow{o} \neq \overrightarrow{b} \in V$, které splňují uvedenou rovnost.*

D ů k a z: Nechť $f$ je endomorfizmus ve $\mathcal{V}$, $M$ je báze prostoru $\mathcal{V}$, $A$ je matice endomorfizmu $f$ vzhledem k $M$ a $\overrightarrow{o} \neq \overrightarrow{b} \in V$. Nechť $f(\overrightarrow{b}) = \lambda_0 \overrightarrow{b}$. Platí

$$\{f(\overrightarrow{b})\}_M = \{\overrightarrow{b}\}_M \cdot A,$$

$$\{\lambda_0 \overrightarrow{b}\}_M = \lambda_0\{\overrightarrow{b}\}_M = \{\overrightarrow{b}\}_M \cdot \lambda_0 E,$$

proto $\{\overrightarrow{b}\}_M \cdot A = \{\overrightarrow{b}\}_M \cdot \lambda_0 E$, a tedy

$$\{\overrightarrow{b}\}(A - \lambda_0 E) = \overrightarrow{o}.$$

Pak také platí

$$(A^T - \lambda_0 E)\overrightarrow{b}^T = \overrightarrow{o}^T,$$

tedy soustava lineárních rovnic $(A^T - \lambda_0 E)\overrightarrow{\xi}^T = \overrightarrow{o}^T$ má netriviální řešení $\overrightarrow{b}$. Dostáváme tak, že $\det(A^T - \lambda_0 E) = 0$, a odtud také $\det(A - \lambda_0 E) = 0$. Proto $\lambda_0$ je vlastním číslem endomorfizmu $f$.

Obráceně, nechť $\lambda_0$ je vlastním číslem $f$. Pak $\det(A - \lambda_0 E) = 0$, proto existuje netriviální řešení $\overrightarrow{b}$ soustavy $(A^T - \lambda_0 E)\overrightarrow{\xi}^T = \overrightarrow{o}^T$. Tj. $(A^T - \lambda_0 E)\overrightarrow{b}^T = \overrightarrow{o}^T$, neboli $A^T \overrightarrow{b}^T = \lambda_0 E \overrightarrow{b}^T$. Tedy $\overrightarrow{b} A = \overrightarrow{b} \cdot \lambda_0 E$, a proto $\{\overrightarrow{b}\}_M \cdot A = \lambda_0 \{\overrightarrow{b}\}_M$. Ovšem $\{\overrightarrow{b}\}_M \cdot A = \{f(\overrightarrow{b})\}_M$, takže dostáváme $f(\overrightarrow{b}) = \lambda_0 \overrightarrow{b}$. □

**Věta 11.17** *Jestliže $f$ je endomorfizmus prostoru $\mathcal{V}$, pak vlastní vektory endomorfizmu $f$, které odpovídají jeho různým vlastním číslům, jsou lineárně nezávislé.*

D ů k a z: Nechť $\lambda_1, \dots, \lambda_m$ jsou navzájem různá vlastní čísla endomorfizmu $f$ a nechť $\overrightarrow{b_1}, \dots, \overrightarrow{b_m}$ jsou vlastní vektory, které jim postupně přísluší.

Důkaz povedeme matematickou indukcí. Pro $m = 1$ je situace zřejmá. Předpokládejme proto, že $m > 1$ a že už platí, že vektory $\overrightarrow{b_1}, \dots, \overrightarrow{b_{m-1}}$ jsou lineárně nezávislé. Nechť $\alpha_1, \dots, \alpha_m \in T$ jsou takové, že

$$\alpha_1 \overrightarrow{b_1} + \ldots + \alpha_{m-1}\overrightarrow{b_{m-1}} + \alpha_m \overrightarrow{b_m} = \overrightarrow{o}. \tag{11.1}$$

Pak, protože $f$ je endomorfizmus, platí

$$\alpha_1 f(\overrightarrow{b_1}) + \ldots + \alpha_{m-1} f(\overrightarrow{b_{m-1}}) + \alpha_m f(\overrightarrow{b_m}) = f(\overrightarrow{o}) = \overrightarrow{o},$$

tedy

$$\alpha_1\lambda_1 \overrightarrow{b_1} + \ldots + \alpha_{m-1}\lambda_{m-1}\overrightarrow{b_{m-1}} + \alpha_m\lambda_m \overrightarrow{b_m} = \overrightarrow{o}. \tag{11.2}$$

Po vynásobení rovnosti 11.1 číslem $\lambda_m$ dostáváme

$$\alpha_1\lambda_m \overrightarrow{b_1} + \ldots + \alpha_{m-1}\lambda_m\overrightarrow{b_{m-1}} + \alpha_m\lambda_m \overrightarrow{b_m} = \overrightarrow{o},$$

tedy

$$\alpha_m \lambda_m \overrightarrow{b_m} = -\alpha_1 \lambda_m \overrightarrow{b_1} - \ldots - \alpha_{m-1} \lambda_m \overrightarrow{b_{m-1}}.$$

Dosazením do 11.2 tak získáme rovnost

$$\alpha_1 \lambda_1 \overrightarrow{b_1} + \ldots + \alpha_{m-1} \lambda_{m-1} \overrightarrow{b_{m-1}} - \alpha_1 \lambda_m \overrightarrow{b_1} - \ldots - \alpha_{m-1} \lambda_m \overrightarrow{b_{m-1}} = \overrightarrow{o},$$

tedy

$$\alpha_1 (\lambda_1 - \lambda_m) \overrightarrow{b_1} + \ldots + \alpha_{m-1} (\lambda_{m-1} - \lambda_m) \overrightarrow{b_{m-1}} = \overrightarrow{o}.$$

Ovšem vektory $\overrightarrow{b_1}, ..., \overrightarrow{b_{m-1}}$ jsou podle předpokladu lineárně nezávislé a $\lambda_1, ..., \lambda_{m-1}$ jsou navzájem různá čísla, proto dostáváme, že $\alpha_1 = ... = \alpha_{m-1} = 0$. Tedy podle 11.1 platí $\alpha_m \overrightarrow{b_m} = \overrightarrow{o}$, a protože $\overrightarrow{b_m} \neq \overrightarrow{o}$, musí platit také $\alpha_m = 0$. Proto jsou vektory $\overrightarrow{b_1}, \ldots, \overrightarrow{b_m}$ lineárně nezávislé. □

**Příklad 11.1** Nechť $f$ je endomorfizmus aritmetického vektorového prostoru $\mathcal{R}^3$, který má vzhledem k některé bázi v $\mathcal{R}^3$ matici

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

Určete vlastní čísla a vlastní vektory endomorfizmu $f$.

Nejdříve najdeme charakteristický polynom.

$$\det(A - \lambda E) = \begin{vmatrix} 3-\lambda & 3 & 2 \\ 1 & 1-\lambda & -2 \\ -3 & -1 & -\lambda \end{vmatrix} = \begin{vmatrix} 3-\lambda & 3 & 2 \\ 4-\lambda & 4-\lambda & 0 \\ -3 & -1 & -\lambda \end{vmatrix} =$$

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

Prostor $\mathcal{R}^3$ je vektorovým prostorem nad tělesem $\mathcal{R}$ a charakteristický polynom má jediný reálný kořen $\lambda_1 = 4$, proto také $f$ má jediné vlastní číslo $\lambda_1 = 4$.

Podprostor vlastních vektorů příslušných k $\lambda_1$ získáme jako množinu řešení homogenní soustavy lineárních rovnic $\overrightarrow{b}(A - 4E) = \overrightarrow{o}$, kterou můžeme také přepsat do tvaru $(A^T - 4E)\overrightarrow{b}^T = \overrightarrow{o}^T$. Dostáváme soustavu

$$\begin{pmatrix} -1 & 1 & -3 \\ 3 & -3 & -1 \\ 2 & -2 & -4 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

která má obecné řešení ve tvaru $(b_1, b_1, 0)$, kde $b_1 \in \mathbb{R}$. Tedy $W_{\lambda_1} = [\{(1, 1, 0)\}]$.

## 11.4 Cvičení

**11.1** Určete defekty a hodnosti následujících homomorfizmů vektorových prostorů

a) $f : \mathcal{R}^2 \longrightarrow \mathcal{R}^2, f((x_1, x_2)) = (2x_1 + x_2, x_1 + x_2)$.

b) $f : \mathcal{R}^3 \longrightarrow \mathcal{R}^4, f((x_1, x_2, x_3)) = (x_1, x_1, x_1, x_1)$.

c) $f : \mathcal{R}^4 \longrightarrow \mathcal{R}, f((x_1, x_2, x_3, x_4)) = (x_1 + x_2 + x_3 + x_4)$.

d) $f : T^2 \longrightarrow T^n, f((x_1, x_2)) = (x_1, x_2, x_1, x_2, \ldots)$.

[ a) $\dim \operatorname{Ker} f = 0$, $\dim \operatorname{Im} f = 2$; b) $\dim \operatorname{Ker} f = 2$, $\dim \operatorname{Im} f = 1$; c) $\dim \operatorname{Ker} f = 3$, $\dim \operatorname{Im} f = 1$; c) $\dim \operatorname{Ker} f = 0$, $\dim \operatorname{Im} f = 2$ ]

**11.2** Určete matici endomorfizmu $f$ aritmetického vektorového prostoru $\mathcal{R}^3$ takového, že

$$f((x_1, x_2, x_3)) = (x_1 + x_2, x_2 + x_3, x_1 + x_3),$$

vzhledem

a) ke kanonické bázi;

b) k bázi $M = \{\overrightarrow{u_1}, \overrightarrow{u_2}, \overrightarrow{u_3}\}$, kde $\overrightarrow{u_1} = (1, -1, 1)$, $\overrightarrow{u_2} = (2, 1, -1)$, $\overrightarrow{u_3} = (-3, -2, 1)$.

[ a) $\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$; b) $\begin{pmatrix} \frac{2}{3} & -\frac{10}{3} & -2 \\ \frac{4}{3} & -\frac{2}{3} & -1 \\ -2 & 3 & 3 \end{pmatrix}$. ]

**11.3** Je dána báze $M = \{\overrightarrow{a_1}, \overrightarrow{a_2}, \overrightarrow{a_3}\}$ prostoru $\mathcal{R}^3$ taková, že

$$\overrightarrow{a_1} = (2, 1, 3), \overrightarrow{a_2} = (1, -1, 2), \overrightarrow{a_3} = (1, 0, 2).$$

Nechť

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

je matice endomorfizmu $f$ prostoru $\mathcal{R}^3$ vzhledem k bázi $M$. Určete $f(\overrightarrow{u})$, jestliže

a) $\overrightarrow{u} = (1, 3, 5)$;

b) $\overrightarrow{u} = (5, 1, 4)$.

[ a) $(29, -15, 62)$; b) $(-16, 23, -40)$ ]

**11.4** Nechť $f$ je endomorfizmus prostoru $\mathcal{R}^3$ s maticí

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

vzhledem k některé bázi v $\mathcal{R}^3$. Určete vlastní čísla a vlastní vektory endomorfizmu $f$.

[ $\lambda_1 = -4$, $\lambda_2 = 3$, $\lambda_3 = 1$, $\mathcal{W}_{\lambda_1} = [\{(-3, 5, 1)\}]$, $\mathcal{W}_{\lambda_2} = [\{(3, 2, -1)\}]$, $\mathcal{W}_{\lambda_3} = [\{(1, 0, 3)\}]$ ]

**11.5** Určete vlastní čísla a vlastní vektory endomorfizmu $g$ prostoru $\mathcal{R}^4$, který má vzhledem k dané bázi matici

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

[ $\lambda_1 = 2$, $\lambda_2 = -2$, $\mathcal{W}_{\lambda_1} = [\{\overrightarrow{u_1}, \overrightarrow{u_2}, \overrightarrow{u_3}\}]$, kde $\overrightarrow{u_1} = (1,1,0,0)$, $\overrightarrow{u_2} = (1,0,1,0)$, $\overrightarrow{u_3} = (1,0,0,1)$, $\mathcal{W}_{\lambda_2} = [\{(1,-1,-1,-1)\}]$ ]

# Kapitola 12

# Endomorfizmy eukleidovských vektorových prostorů

Připomeňme si, že eukleidovským vektorovým prostorem rozumíme libovolný vektorový prostor $\mathcal{V}$ nad tělesem reálných čísel $\mathcal{R}$ uvažovaný spolu s některým skalárním součinem. Jestliže $\overrightarrow{x}, \overrightarrow{y} \in V$, pak jejich skalární součin $\langle \overrightarrow{x}, \overrightarrow{y} \rangle$ budeme v dalším textu zapisovat jednodušeji ve tvaru $\overrightarrow{x} \cdot \overrightarrow{y}$. Jestliže $\mathcal{V} = \mathcal{R}^n$ pak budeme předpokládat, že používáme obyčejný skalární součin, tj. pro $\overrightarrow{x} = (x_1, \dots, x_n)$, $\overrightarrow{y} = (y_1, \dots, y_n)$ je $\overrightarrow{x} \cdot \overrightarrow{y} = \sum\limits_{i=1}^{n} x_i \cdot y_i$.

## 12.1 Ortogonální matice a ortogonální endomorfizmy eukleidovských vektorových prostorů

**Definice 12.1** *Jestliže $A \in M_n(\mathcal{R})$, pak matice $A$ se nazývá* ortogonální, *platí-li*

$$A \cdot A^T = E = A^T \cdot A.$$

`Poznámka:` $A$ je tedy ortogonální matice právě tehdy, když $A^T = A^{-1}$. Odtud také dostáváme, že každá ortogonální matice je regulární.

**Věta 12.1** *Pro libovolnou matici $A \in M_n(\mathcal{R})$ jsou následující podmínky ekvivalentní.*

*a) $A$ je ortogonální.*

*b) Řádky matice $A$ tvoří v $\mathcal{R}^n$ ortonormální systém vektorů.*

*c) Sloupce matice $A$ tvoří v $(\mathcal{R}^n)^T$ ortonormální systém vektorů.*

D ů k a z: 1 $\Leftrightarrow$ 2: Jestliže matice $A$ je ortogonální, pak $A \cdot A^T = E$. Tedy jsou-li $\overrightarrow{a_i}$ a $\overrightarrow{a_j}$ $i$-tý a $j$-tý řádek v $A$, platí $\overrightarrow{a_i} \cdot \overrightarrow{a_j} = 1$ pro $i = j$ a $\overrightarrow{a_i} \cdot \overrightarrow{a_j} = 0$ pro $i \neq j$. Stejně snadno je vidět obrácená implikace.

1 $\Leftrightarrow$ 3: Zde se analogicky využije rovnost $A^T \cdot A = E$ z definice ortogonální matice. $\square$

**Věta 12.2**

*a) Inverzní matice k ortogonální matici je ortogonální.*

*b) Součin ortogonálních matic je ortogonální matice.*

*c) Matice přechodu od ortonormální báze k ortonormální bázi je ortogonální.*

D ů k a z:

a) Nechť $A$ je ortogonální matice. Pak $(A^{-1})^T \cdot A^{-1} = (A^T)^{-1} \cdot A^{-1} = (AA^T)^{-1} = E$, a podobně $A^{-1} \cdot (A^{-1})^T = E$.

b) Nechť $A$ a $B$ jsou ortogonální matice. Pak

$$AB \cdot (AB)^T = ABB^T A^T = E = (AB)^T \cdot AB.$$

c) Nechť $M = \{\overrightarrow{e_1}, \ldots, \overrightarrow{e_n}\}$ a $M' = \{\overrightarrow{e_1}', \ldots, \overrightarrow{e_n}'\}$ jsou dvě ortonormální báze ve $\mathcal{V}$ a nechť $A = ||a_{ij}||$ je matice přechodu od $M$ k $M'$. Pak

$$\overrightarrow{e_i}' \cdot \overrightarrow{e_j}' = \left(\sum_{k=1}^{n} a_{ik}\overrightarrow{e_k}\right) \cdot \left(\sum_{l=1}^{n} a_{jl}\overrightarrow{e_l}\right) = \sum_{k,l=1}^{n} a_{ik}a_{jl}\overrightarrow{e_k}\overrightarrow{e_l} = \sum_{k=1}^{n} a_{ik}a_{jk},$$

tedy $\overrightarrow{e_i}' \cdot \overrightarrow{e_j}' = 1$ pro $i = j$, a $\overrightarrow{e_i}' \cdot \overrightarrow{e_j}' = 0$ pro $i \neq j$.

□

**Definice 12.2** *Endomorfizmus $f$ eukleidovského vektorového prostoru $\mathcal{V}$ se nazývá* ortogonální, *jestliže pro libovolné vektory $\overrightarrow{x}, \overrightarrow{y} \in V$ platí $f(\overrightarrow{x}) \cdot f(\overrightarrow{x}) = \overrightarrow{x} \cdot \overrightarrow{y}$. (Později ukážeme, že každý ortogonální endomorfizmus je bijektivní, a že je to tedy izomorfizmus eukleidovského vektorového prostoru $\mathcal{V}$ do $\mathcal{V}$.)*

**Věta 12.3** *Endomorfizmus $f$ eukleidovského vektorového prostoru $\mathcal{V}$ je ortogonální, právě když pro každý vektor $\overrightarrow{x} \in V$ platí, že $f(\overrightarrow{x}) \cdot f(\overrightarrow{x}) = \overrightarrow{x} \cdot \overrightarrow{x}$, tedy když $f$ zachovává délky vektorů.*

D ů k a z: Jestliže $f$ je ortogonální endomorfizmus, pak zachovává skalární součiny, a proto $f$ zachovává také délky vektorů.

Dokážeme proto obrácenou implikaci. Nechť endomorfizmus $f$ zachovává délky vektorů a nechť $\overrightarrow{a}, \overrightarrow{b} \in V$. Jestliže $f(\overrightarrow{a}) = \overrightarrow{a}'$ a $f(\overrightarrow{b}) = \overrightarrow{b}'$ pak $f(\overrightarrow{a} + \overrightarrow{b}) = \overrightarrow{a}' + \overrightarrow{b}'$. Podle předpokladu tedy platí $(\overrightarrow{a} + \overrightarrow{b}) \cdot (\overrightarrow{a} + \overrightarrow{b}) = (\overrightarrow{a}' + \overrightarrow{b}') \cdot (\overrightarrow{a}' + \overrightarrow{b}')$, a odtud

$$\overrightarrow{a} \cdot \overrightarrow{a} + 2\overrightarrow{a} \cdot \overrightarrow{b} + \overrightarrow{b} \cdot \overrightarrow{b} = \overrightarrow{a}' \cdot \overrightarrow{a}' + 2\overrightarrow{a}' \cdot \overrightarrow{b}' + \overrightarrow{b}' \cdot \overrightarrow{b}'.$$

Protože $\overrightarrow{a} \cdot \overrightarrow{a} = \overrightarrow{a}' \cdot \overrightarrow{a}'$ a $\overrightarrow{b} \cdot \overrightarrow{b} = \overrightarrow{b}' \cdot \overrightarrow{b}'$, dostáváme $\overrightarrow{a} \cdot \overrightarrow{b} = \overrightarrow{a}' \cdot \overrightarrow{b}'$, neboli $\overrightarrow{a} \cdot \overrightarrow{b} = f(\overrightarrow{a}) \cdot f(\overrightarrow{b})$. □

**Věta 12.4** *Nechť $f$ je endomorfizmus eukleidovského vektorového prostoru $\mathcal{V}$ a nechť $M = \{\overrightarrow{e_1}, \dots, \overrightarrow{e_n}\}$ je libovolná báze ve $\mathcal{V}$. Pak $f$ je ortogonální, právě když $f(\overrightarrow{e_i}) \cdot f(\overrightarrow{e_j}) = \overrightarrow{e_i} \cdot \overrightarrow{e_j}$ pro každé $i, j \in \{1, \dots, n\}$.*

D ů k a z: Nechť endomorfizmus $f$ splňuje podmínku na pravé straně dokazované ekvivalence, tedy nechť zachovává skalární součin pro vektory z $M$. Předpokládejme, že $\overrightarrow{a} \in V$ a že $\overrightarrow{a} = \sum_{i=1}^{n} \alpha_i \overrightarrow{e_i}$. Pak

$$f(\overrightarrow{a}) \cdot f(\overrightarrow{a}) = \sum_{i,j=1}^{n} \alpha_i \alpha_j f(\overrightarrow{e_i}) \cdot f(\overrightarrow{e_j}) = \sum_{i,j=1}^{n} \alpha_i \alpha_j \cdot \overrightarrow{e_i} \overrightarrow{e_j} = \overrightarrow{a} \cdot \overrightarrow{a}.$$

Tedy $f$ zachovává délky vektorů, a proto podle věty 12.4 $f$ je ortogonální endomorfizmus prostoru $\mathcal{V}$.

Obrácená implikace je triviální. □

V dalších větách ukážeme těsné vztahy mezi ortogonálními endomorfizmy, ortogonálními maticemi a ortonormálními bázemi.

**Věta 12.5**

a) *Ortogonální endomorfizmus převádí libovolnou ortonormální bázi na ortonormální bázi.*

b) *Jestliže endomorfizmus $f$ převádí některou ortonormální bázi na ortonormální bázi, pak $f$ je ortogonální.*

D ů k a z:

a) Nechť $f$ je ortogonální endomorfizmus a nechť $M = \{\overrightarrow{e_1}, \dots, \overrightarrow{e_n}\}$ je ortonormální báze. Pak $f(\overrightarrow{e_i}) \cdot f(\overrightarrow{e_j}) = \overrightarrow{e_i} \cdot \overrightarrow{e_j}$ pro každé $i, j \in \{1, \dots, n\}$, proto $M' = \{f(\overrightarrow{e_1}), \dots, f(\overrightarrow{e_n})\}$ je ortonormální báze.

b) Nechť $f$ je endomorfizmus a nechť existuje ortonormální báze $M = \{\overrightarrow{e_1}, \dots, \overrightarrow{e_n}\}$ taková, že $M' = \{f(\overrightarrow{e_1}), \dots, f(\overrightarrow{e_n})\}$ je ortonormální báze. Pak $f(\overrightarrow{e_i}) \cdot f(\overrightarrow{e_j}) = \overrightarrow{e_i} \cdot \overrightarrow{e_j}$ pro každé $i, j \in \{1, \dots, n\}$, a proto podle věty 12.4 $f$ je ortogonální.

□

**Věta 12.6**

a) *Matice ortogonálního endomorfizmu vzhledem k libovolné ortonormální bázi je ortogonální.*

b) *Jestliže matice endomorfizmu $f$ je vzhledem k některé ortonormální bázi ortogonální, pak $f$ je ortogonální endomorfizmus.*

D ů k a z:

a) Nechť $f$ je endomorfizmus, $M = \{\overrightarrow{e_1}, \dots, \overrightarrow{e_n}\}$ ortonormální báze a nechť $A = ||a_{ij}||$ je matice $f$ vzhledem k $M$. Pak

$$f(\overrightarrow{e_i}) \cdot f(\overrightarrow{e_j}) = \left(\sum_{k=1}^{n} a_{ik} \overrightarrow{e_k}\right) \cdot \left(\sum_{l=1}^{n} a_{jl} \overrightarrow{e_l}\right) = \sum_{k=1}^{n} a_{ik} a_{jk}.$$

Tedy jestliže $f$ je ortogonální, platí $f(\overrightarrow{e_i}) \cdot f(\overrightarrow{e_j}) = \overrightarrow{e_i} \cdot \overrightarrow{e_j}$, proto $f(\overrightarrow{e_i}) \cdot f(\overrightarrow{e_j}) = 0$ pro $i \neq j$ a $f(\overrightarrow{e_i}) \cdot f(\overrightarrow{e_j}) = 1$ pro $i = j$.

b) Podle části a) důkazu platí

$$f(\overrightarrow{e_i}) \cdot f(\overrightarrow{e_j}) = \sum_{k=1}^{n} a_{ik} a_{jk}$$

pro libovolný endomorfizmus $f$. Proto pokud matice $A$ je ortogonální, platí $\varphi(\overrightarrow{e_i}) \cdot \varphi(\overrightarrow{e_j}) = 0$ pro $i \neq j$ a $\varphi(\overrightarrow{e_i}) \cdot \varphi(\overrightarrow{e_j}) = 1$ pro $i = j$, tzn., že vždy dostáváme $\varphi(\overrightarrow{e_i}) \cdot \varphi(\overrightarrow{e_j}) = \overrightarrow{e_i} \cdot \overrightarrow{e_j}$. Podle věty 12.4 tak platí, že endomorfizmus $f$ je ortogonální.

□

`Poznámka`: Protože každá ortogonální matice je regulární, dostáváme tak, že každý ortogonální endomorfizmus je vlastně izomorfizmus eukleidovských vektorových prostorů.

## 12.2 Symetrické matice a symetrické endomorfizmy eukleidovských vektorových prostorů

**Definice 12.3** *Endomorfizmus $f$ eukleidovského vektorového prostoru $\mathcal{V}$ se nazývá* symetrický, *jestliže pro libovolné $\overrightarrow{x}, \overrightarrow{y} \in V$ platí*

$$f(\overrightarrow{x}) \cdot \overrightarrow{y} = \overrightarrow{x} \cdot f(\overrightarrow{y}).$$

**Definice 12.4** *Jestliže $A \in M_n(\mathcal{R})$, pak $A$ se nazývá* symetrická matice, *platí-li $A^T = A$.*

**Věta 12.7** *Endomorfizmus $f$ eukleidovského prostoru $\mathcal{V}$ je symetrický právě tehdy, když pro některou bázi $M = \{\overrightarrow{e_1}, \dots, \overrightarrow{e_n}\}$ prostoru $\mathcal{V}$ platí*

$$f(\overrightarrow{e_i}) \cdot \overrightarrow{e_j} = \overrightarrow{e_i} \cdot f(\overrightarrow{e_j}),$$

*pro každé $i, j \in \{1, \dots, n\}$.*

D ů k a z: Jestliže $f$ je symetrický, pak samozřejmě splňuje podmínku z věty.

Nechť tedy obráceně $f$ splňuje uvedenou podmínku pro některou bázi $M = \{\overrightarrow{e_1}, \dots, \overrightarrow{e_n}\}$ ve $\mathcal{V}$ a nechť $\overrightarrow{a}$ a $\overrightarrow{b}$ jsou libovolné vektory z $\mathcal{V}$. Předpokládejme, že $\overrightarrow{a} = \sum_{i=1}^{n} \alpha_i \overrightarrow{e_i}$, $\overrightarrow{b} = \sum_{i=1}^{n} \beta_i \overrightarrow{e_i}$. Pak

$$f(\overrightarrow{a}) \cdot \overrightarrow{b} = \left(\sum_{i=1}^{n} \alpha_i f(\overrightarrow{e_i})\right)\left(\sum_{j=1}^{n} \beta_j \overrightarrow{e_j}\right) = \sum_{i,j=1}^{n} \alpha_i \beta_j f(\overrightarrow{e_i}) \cdot \overrightarrow{e_j} = \sum_{i,j=1}^{n} \alpha_i \beta_j \cdot \overrightarrow{e_i} \cdot f(\overrightarrow{e_j}),$$

$$\overrightarrow{a} \cdot f(\overrightarrow{b}) = \left(\sum_{i=1}^{n} \alpha_i \overrightarrow{e_i}\right)\left(\sum_{j=1}^{n} \beta_j f(\overrightarrow{e_j})\right) = \sum_{i,j=1}^{n} \alpha_i \beta_j \cdot \overrightarrow{e_i} \cdot f(\overrightarrow{e_j}),$$

tedy $f(\overrightarrow{a}) \cdot \overrightarrow{b} = \overrightarrow{a} \cdot f(\overrightarrow{b})$, a proto endomorfizmus $f$ je symetrický. □

**Věta 12.8**

*a) Symetrický endomorfizmus má vzhledem k libovolné ortonormální bázi symetrickou matici.*

*b) Má-li endomorfizmus $f$ eukleidovského prostoru vzhledem k některé ortonormální bázi symetrickou matici, pak $f$ je symetrický.*

D ů k a z:

a) Nechť $\mathcal{V}$ je eukleidovský prostor, $f$ jeho symetrický endomorfizmus, $M = \{\overrightarrow{e_1}, \dots, \overrightarrow{e_n}\}$ ortonormální báze ve $\mathcal{V}$ a nechť $A = ||\alpha_{ij}||$ je matice endomorfizmu $f$ vzhledem k $M$. Pak pro libovolná $i, j \in \{1, \dots, n\}$ platí $f(\overrightarrow{e_i}) \cdot \overrightarrow{e_j} = \overrightarrow{e_i} \cdot f(\overrightarrow{e_j})$, a protože

$$f(\overrightarrow{e_i}) \cdot \overrightarrow{e_j} = \left(\sum_{k=1}^{n} \alpha_{ik} \overrightarrow{e_k}\right) \cdot \overrightarrow{e_j} = \alpha_{ij},$$

$$\overrightarrow{e_i} \cdot f(\overrightarrow{e_j}) = \overrightarrow{e_i} \cdot \left(\sum_{k=1}^{n} \alpha_{jk} \overrightarrow{e_k}\right) = \alpha_{ji},$$

dostáváme $\alpha_{ij} = \alpha_{ji}$, tedy matice $A$ je symetrická.

b) Jestliže endomorfizmus $f$ prostoru $\mathcal{V}$ má vzhledem k některé ortonormální bázi symetrickou matici $A = ||\alpha_{ij}||$, pak $\alpha_{ij} = \alpha_{ji}$ pro každá $i, j \in \{1, \dots, n\}$, a proto z rovností odvozených v a) dostáváme, že vždy

$$f(\overrightarrow{e_i}) \cdot \overrightarrow{e_j} = \overrightarrow{e_i} \cdot f(\overrightarrow{e_j}).$$

Tedy podle věty 12.7 platí, že endomorfizmus $f$ je symetrický. □

Připomeňme, že je-li $\mathcal{V}$ vektorový prostor nad číselným tělesem $\mathcal{T}$ a $f$ je endomorfizmus prostoru $\mathcal{V}$, pak vlastní čísla endomorfizmu $f$ jsou čísla z $\mathcal{T}$, která jsou kořeny charakteristického polynomu endomorfizmu $f$. Přitom každý polynom $n$-tého stupně s koeficienty z $\mathcal{T}$ má v $\mathcal{T}$ nejvýše $n$ kořenů (počítaných s násobností).

Viděli jsme např., že endomorfizmus aritmetického vektorového prostoru $\mathcal{R}^3$ může mít méně než tři vlastní čísla. Platí ale, že každý polynom $n$-tého stupně ($n \geq 1$) s koeficienty z číselného tělesa $\mathcal{T}$ má v tělese komplexních čísel $\mathcal{C}$ právě $n$ kořenů počítaných s násobností.

Proto budeme obecněji za *vlastní číslo endomorfizmu* vektorového prostoru nad $\mathcal{T}$ považovat každý z komplexních kořenů charakteristického polynomu toho endomorfizmu.

Pak pro symetrické endomorfizmy eukleidovských vektorových prostorů platí následující věta.

**Věta 12.9** *Všechna vlastní čísla symetrického endomorfizmu eukleidovského vektorového prostoru jsou reálná.*

D ů k a z: Nechť $\mathcal{V}$ je eukleidovský vektorový prostor, $f$ je jeho symetrický endomorfizmus a nechť $A = ||\alpha_{ij}|| \in M_n(\mathcal{R})$ je matice $f$ vzhledem k některé ortonormální bázi ve $\mathcal{V}$. Podle věty 12.8 platí, že matice $A$ je symetrická. Předpokládejme že $\lambda_0 \in \mathbb{C}$ je vlastní číslo endomorfizmu $f$. Pak $\det(A - \lambda_0 E) = 0$, a tedy homogenní soustava $(A - \lambda_0 E)\overrightarrow{\xi}^T = \overrightarrow{o}^T$ má nad $\mathcal{C}$ netriviální řešení, např. $\overrightarrow{y} = (y_1, \ldots, y_n)$. Tedy

$$\sum_{j=1}^{n} \alpha_{ij} y_j = \lambda_0 y_i, \forall i \in \{1, \ldots, n\}.$$

Vynásobíme obě strany $i$-té rovnosti ($i = 1, \ldots, n$) číslem $\overline{y_i}$ komplexně sdruženým s $y_i$. Po sečtení všech vynásobených rovností dostaneme

$$\sum_{i,j=1}^{n} \alpha_{ij} y_j \overline{y_i} = \lambda_0 \sum_{i=1}^{n} y_i \overline{y_i}.$$

Platí, že $0 < \sum\limits_{i=1}^{n} y_i \overline{y_i} \in \mathbb{R}$. Proto k důkazu toho, že $\lambda_0 \in \mathbb{R}$, stačí ověřit, že také levá strana v poslední rovnosti patří do $\mathbb{R}$. Dostáváme postupně:

$$\overline{\sum_{i,j=1}^{n} \alpha_{ij} y_j \overline{y_i}} = \sum_{i,j=1}^{n} \overline{\alpha_{ij} y_i \overline{y_j}} = \sum_{i,j=1}^{n} \alpha_{ij} \overline{y_j} y_i = \sum_{i,j=1}^{n} \alpha_{ji} \overline{y_j} y_i = \sum_{i,j=1}^{n} \alpha_{ij} \overline{y_i} y_j = \sum_{i,j=1}^{n} \alpha_{ij} y_j \overline{y_i},$$

tedy číslo $\sum\limits_{i,j=1}^{n} \alpha_{ij} y_j \overline{y_i}$ se rovná číslu, které je s ním komplexně sdružené, a proto patří do $\mathbb{R}$. Tedy $\lambda_0 \in \mathbb{R}$. □

# Výběr z literatury


[1] Bečvář, J. *Sbírka úloh z lineární algebry (skriptum)*, (1975 Praha).

[2] Bican, L. *Lineární algebra*, (1979 Praha)

[3] Birkhoff, G., Mac Lane, S. *Prehľad modernej algebry*, (1979 Bratislava).

[4] Blažek, J., Calda, E., Koman, M., Kussová, B. *Algebra a teoretická aritmetika I*, (1983 Praha).

[5] Blažek, J., Koman, M., Vojtášková, B. *Algebra a teoretická aritmetika II*, (1985 Praha).

[6] Katriňák, T. a kol. *Algebra a teoretická aritmetika (1)*, (1985 Bratislava).

[7] Proskurjakov, I. V. *Sbornik zadač po linějnoj algebre*, (1970 Moskva).

[8] Šalát, T. a kol. *Algebra a teoretická aritmetika (2)*, (1986 Bratislava).

[9] Šik, F. *Lineární algebra zaměřená na numerickou analýzu*, (1998 Brno).

# Index

# Obsah