ZÁKLADY MATEMATIKY I

Katedra aplikované matematiky a informatiky
Ekonomicko-správní fakulta MU v Brně
Email: `vesely@econ.muni.cz`
http://www.math.muni.cz/~vesely

OBSAH

Date: 6. prosince 2006.

- Systémy lineárních rovnic. Cramerovo pravidlo, eliminační metody. Frobeniova věta.
- Popis množiny všech řešení pro homogenní i nehomogenní systémy.
- Transformace souřadnic a diagonalizace matic.

Literatura ke studiu

Základní:

[KaSk] Karásek J., Skula L.: Algebra a geometrie, PC-DIR Real s.r.o., Brno 2002 (skripta VUT Brno, Fakulta strojního inženýrství)

[Šik] Šik F.: Lineární algebra zaměřená na numerickou analýzu, PřF MU Brno, 1998 (skripta)

[Ho] Horák P.: Cvičení z algebry a teoretické aritmetiky I., PřF MU Brno, 2002 (sbírka řešených i neřešených úloh)

- Pracovní texty vytvořené přednášejícím, které jsou ke stažení v elektronické podobě z IS MU u příslušného předmětu.

Doplňující:

[Mi] Minorskij V.P.: Sbírka úloh z vyšší matematiky, SNTL Praha, 1964

[FaSo] Faddejev A.K.,Sominskij J.S.: Zbierka úloh z vyššej algebry, ALFA Bratislava, 1968

Poznámka: V tomto textu jsou úseky látky (definice, věty, důkazy a pod.) z hlediska důležitosti rozlišeny ve třech úrovních změnou sazby příslušného klíčového slova takto:

1. **Základní:** podtrženě velkými písmeny (např. <u>**VĚTA**</u>).
2. **Důležité:** velkými písmeny (např. **VĚTA**).
3. **Doplňující:** jsou vysázeny obyčejně (např. **Věta**).

U důkazů stačí vyložit podstatné myšlenky (postup) vlastními slovy.

1.1. ZÁKLADY VÝROKOVÉHO POČTU.

Teorie: `[KaSk: s.7-9]`
Příklady: `[Ho:řešené č.1; s.5-6]`, `[Ho:neřešené §1; s.39-42]`

Matematické vyjadřování:

- **Stručnost**: užívání symbolů (viz přílohu C)
- **Přesnost**: definice, tvrzení, pomocné tvrzení (lemma), věta (teorém), poznámka, seznam označení: $s := v$ nebo $v =: s$ interpretujeme jako označení výrazu v symbolem s.

Účelem **definice** je přesné vymezení významu nově zaváděného matematického pojmu.

Účelem **tvrzení**, mezi něž patří **lemmata** i **věty** (důležitá tvrzení), je vyvodit z výchozích předpokladů přesné logické závěry postupnou aplikací **logických pravidel**. Tomuto postupu říkáme **důkaz**. Univerzální předpoklady matematických teorií se nazývají **axiomy**: vyjadřují předem dané skutečnosti, které považujeme za univerzálně platné.

Výroky: při užití logických pravidel vystupuje jeden ze základních pojmů logiky — pojem **výroku**.

Výrokem rozumíme libovolné sdělení (tvrzení), o kterém má smysl říci, jestli je pravdivé nebo nepravdivé. Říkáme také, že výrok **platí** nebo **neplatí**.

Logická hodnota 1 značí výrok, který je vždy pravdivý a podobně **logická hodnota 0** značí výrok, který je vždy nepravdivý. Výroky v dalším budeme označovat symbolicky, například V. Pokud výrok závisí na dalších proměnných (obvykle opět výrocích) $A, B, \ldots$, píšeme $V(A), V(A,B)$ a podobně.

Výrokový počet:

kalkulus s výroky, kdy pomocí logických operací v tzv. **výrokových formulích** konstruujeme **složené výroky** ze zadaných **elementárních výroků** vystupujících v roli operandů. Základní operace jsou popsány pomocí pravdivostních (0–1) tabulek, které každé kombinaci pravdivostních hodnot elementárních výroků přiřazují pravdivostní hodnotu výsledného složeného výroku:

Operace **negace**: $\neg$, $'$

A	$\neg A$
0	1
1	0

Slovní vyjádření: A neplatí

Operace **implikace**: $\Rightarrow$

A	B	$A \Rightarrow B$
0	0	1
0	1	1
1	0	0
1	1	1

Slovní vyjádření: A implikuje B; B plyne z A; B je důsledkem A; A je postačující podmínka pro B; B je nutná podmínka pro A; jestliže platí A, pak platí B.

Operace **ekvivalence**: $\Leftrightarrow$, $\equiv$

A	B	$A \Leftrightarrow B$
0	0	1
0	1	0
1	0	0
1	1	1

Slovní vyjádření: A je ekvivalentní s B; A je nutná a postačující podmínka pro B; B je nutná a postačující podmínka pro A; A platí právě když B platí; A platí tehdy a jen tehdy, když platí B.
Výrok $V(A, B, \dots) \equiv 1$ (vždy pravdivý) se nazývá **tautologie**.

Operace 'A' neboli **logický součin** neboli **konjunkce**: &,$\wedge$

A	B	$A \wedge B = \min(A, B)$
0	0	0
0	1	0
1	0	0
1	1	1

Slovní vyjádření: platí A i B; platí A a B.

Operace 'NEBO' neboli **logický součet** neboli **disjunkce**: $\vee$

A	B	$A \vee B = \max(A, B)$
0	0	0
0	1	1
1	0	1
1	1	1

Slovní vyjádření: platí A nebo B.

Operace 'BUĎ A NEBO': xor

A	B	xor(A, B)
0	0	0
0	1	1
1	0	1
1	1	0

Slovní vyjádření: platí buď A nebo B.

Univerzální kvantifikátor: $\forall$
$\forall x$ *s vlastností* $U : V(x)$
Slovní vyjádření: pro každé x s vlastností U platí $V(x)$.

Existenční kvantifikátor: $\exists$
$\exists x$ *s vlastností* $U : V(x)$
Slovní vyjádření: existuje x s vlastností U splňující $V(x)$.

VĚTA 1.1. *Platí následující ekvivalence výroků:*
(1) $A'' \equiv A$.
(2) $A \wedge B \equiv B \wedge A$, $A \vee B \equiv B \vee A$.
(3) *DeMorganova pravidla:*
$(A \wedge B)' \equiv A' \vee B'$, $(A \vee B)' \equiv A' \wedge B'$.
(4) $(A \Rightarrow B) \equiv (A' \vee B)$, $(A \Rightarrow B) \equiv (B' \Rightarrow A')$.
(5) $(A \not\Rightarrow B) \equiv (A \wedge B')$, $(A \not\Rightarrow B) \equiv (B' \not\Rightarrow A')$.
(6) $(A \Leftrightarrow B) \equiv (A \Rightarrow B) \wedge (B \Rightarrow A), (A \Leftrightarrow B) \equiv (A' \Leftrightarrow B')$.
(7) $(A \not\Leftrightarrow B) \equiv (A \not\Rightarrow B) \vee (B \not\Rightarrow A), (A \not\Leftrightarrow B) \equiv (A' \not\Leftrightarrow B')$.
(8) *Asociativní zákony:*
$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$,
$A \vee (B \vee C) \equiv (A \vee B) \vee C$.
(9) *Distributivní zákony:*
$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$,
$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$.
(10) $(\forall x$ *s vlastností* $U : V(x))' \equiv (\exists x$ *s vlastností* $U : V(x)')$
(11) $(\exists x$ *s vlastností* $U : V(x))' \equiv (\forall x$ *s vlastností* $U : V(x)')$

Poznámka: $A \not\Rightarrow B := (A \Rightarrow B)'$, $A \not\Leftrightarrow B := (A \Leftrightarrow B)'$.

DŮKAZ. CVIČENÍ □

Důkazové techniky:

Matematické věty většinou vyjadřují slovně implikace výroků $A \Rightarrow B$ (A nazýváme předpokladem věty a B tvrzením věty) nebo ekvivalence výroků $A \equiv B$.

Přímý důkaz implikace $A \Rightarrow B$:
konstruujeme posloupnost pravdivých výroků:
$A \Rightarrow A_1, A_1 \Rightarrow A_2, \ldots, A_{n-1} \Rightarrow A_n, A_n \Rightarrow B$, tj. dokazujeme, že je pravdivý výrok $(A \Rightarrow A_1) \wedge (A_1 \Rightarrow A_2) \wedge \cdots \wedge (A_{n-1} \Rightarrow A_n) \wedge (A_n \Rightarrow B)$.

Důkaz implikace $A \Rightarrow B$ sporem:
provádíme přímý důkaz ekvivalentní implikace $B' \Rightarrow A'$, která pak vede ke sporu s platností předpokladu A, pokud by za jeho platnosti tvrzení B neplatilo.

Důkaz ekvivalence $A \Leftrightarrow B$: dokazujeme platnost ekvivalentního výroku (A$\Rightarrow B) \wedge (B \Rightarrow A)$ ve dvou krocích: samostatně dokazujeme platnost obou implikací $A \Rightarrow B$ a $B \Rightarrow A$.

Důkaz platnosti následujícího výroku matematickou indukcí:
$\forall\, n \geq n_0 : V(n)$, kde n, n_0 jsou přirozená čísla.
Nekonečný přímý důkaz tvaru
$V(n_0) \wedge (V(n_0) \Rightarrow V(n_0+1) \Rightarrow V(n_0+2), \ldots)$
nahradíme ověřením platnosti ekvivalentního výroku:
$\forall\, n > n_0 : (V(n_0) \wedge V(n_0+1) \wedge \cdots \wedge V(n-1)) \Rightarrow V(n)$.
Důkaz tak probíhá ve dvou krocích:

- **Počáteční krok**: ověření platnosti výroku $V(n_0)$
- **Indukční krok**: pro každé $n > n_0$ ověříme platnost implikace $(V(n_0) \wedge V(n_0+1) \wedge \cdots \wedge V(n-1)) \Rightarrow V(n)$.

ANGLICKÁ TERMINOLOGIE VÝROKOVÉHO POČTU

definice ♦ definition
tvrzení ♦ statement, proposition
věta ♦ theorem
poznámka ♦ remark
označení ♦ notation
důkaz ♦ proof
axiom ♦ axiom
výrok ♦ sentence, proposition
pravdivý, nepravdivý ♦ true, false
negace ♦ negation
implikace ♦ implication
A implikuje B ♦ A implies B
B plyne z A ♦ B follows from A
B je důsledkem A ♦ B is a consequence of A
A je postačující podmínka pro B ♦ A is a sufficient condition for B
B je nutná podmínka pro A ♦ B is a necessary condition for A
jestliže platí A, pak platí B ♦ if A holds then B holds
tvrzení platí ♦ the statement holds
A je ekvivalentní s B ♦ A is equivalent with B
A je nutná a postačující podmínka pro B ♦ A is a necessary and sufficient condition for B
A platí právě když (tehdy a jen tehdy když) B platí ♦ A holds if and only if (iff) B holds
logický součin: A ♦ logical AND
logický součet: NEBO ♦ (logical) OR
BUĎ ... A NEBO ♦ logical EXCLUSIVE OR, EITHER ... OR
univerzální kvantifikátor ♦ universal quantifier
pro každé x s vlastností U platí $V(x)$ ♦ $V(x)$ is true for all x having property U
existenční kvantifikátor ♦ existential quantifier
existuje x s vlastností U splňující $V(x)$ ♦ there exists x having property U such that $V(x)$ is true

1.2. **ZÁKLADY TEORIE MNOŽIN.**

Teorie a příklady: `[KaSk: s.9-25,37-43]`
Příklady: `[Ho:řešené č.2-4,7-10; s.6-12]`,
`[Ho:neřešené kap.1§2§5; s.42-45,51-54]`

DEFINICE 1.2 (Naivní pojetí teorie množin: Cantor 1849–1918)**.**
Množinou rozumíme soubor libovolných objektů, které nazýváme prvky této množiny. Množina se nazývá **konečná**, resp. **nekonečná**, jestliže má **konečně**, resp. **nekonečně** mnoho prvků.
Zapisujeme:
$a \in A$, $A \ni a$ . . . a je prvkem A.
$a \notin A$, $A \not\ni a$ . . . a není prvkem A.
$A := \{a_1, a_2, \ldots, a_n\}$ . . . specifikace konečné množiny výčtem prvků.
$A := \{x \,|\, x$ má vlastnost V$\}$ . . . specifikace množiny s prvky majícími vlastnost V, například
$\mathbb{R}^+ := \{x \,|\, x \in \mathbb{R}, x \geq 0\}$ značí množinu všech nezáporných reálných čísel.
$\emptyset := \{\}$ . . . **prázdná množina** neobsahuje žádný prvek.

Výše uvedená definice je příliš široká a vede proto k logickým paradoxům. Nejznámější je **Russelův paradox:**
Definujeme-li $M := \{X \,|\, X$ je množina: $X \notin X\}$, pak pro M mohou nastat jen dvě možnosti, obě vedoucí k logickému sporu:
(1) $M \in M$, což z definice implikuje $M \notin M$, nebo
(2) $M \notin M$, což z definice implikuje $M \in M$.

MNOŽINOVÉ INKLUZE
$A = B$ . . . množiny A a B jsou si rovny, mají-li tytéž prvky.
$A \neq B$ . . . množiny A a B jsou různé, nemají-li tytéž prvky.
$A \subseteq B$, $B \supseteq A$ . . . A je **podmnožinou** B nebo též B je **nadmnožinou** A, jestliže každý prvek A je také prvkem B.
$A \subset B$, $B \supset A$ . . . A je **vlastní podmnožinou** B, jestliže $A \subseteq B$ a současně $A \neq B$, tj. kromě všech prvků z A, existuje v B ještě alespoň jeden další prvek.
Příklad: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

__**VĚTA**__ **1.3.** *Platí $A = B$ tehdy a jen tehdy, když $A \subseteq B$ a $B \subseteq A$.*

__*Označení*__ (Intervaly).
Nechť $a, b \in \mathbb{R}$ jsou daná reálná čísla. Pak **intervalem reálných čísel** nazýváme kteroukoli z níže uvedených podmnožin v $\mathbb{R}$:
$[a, b] := \{x \,|\, x \in \mathbb{R} : a \leq x \leq b\}$... uzavřený interval;
$(a, b) := \{x \,|\, x \in \mathbb{R} : a < x < b\}$... otevřený interval;
$[a, b) := \{x \,|\, x \in \mathbb{R} : a \leq x < b\}$... interval zleva uzavřený a zprava otevřený;
$(a, b] := \{x \,|\, x \in \mathbb{R} : a < x \leq b\}$... interval zleva otevřený a zprava uzavřený;
$(-\infty, \infty) := \mathbb{R}$;
$(-\infty, b) := \{x \,|\, x \in \mathbb{R} : x < b\}$;
$(-\infty, b] := \{x \,|\, x \in \mathbb{R} : x \leq b\}$;
$(a, \infty) := \{x \,|\, x \in \mathbb{R} : a < x\}$;
$[a, \infty) := \{x \,|\, x \in \mathbb{R} : a \leq x\}$.

__ZOBRAZENÍ__

__**DEFINICE**__ **1.4.** Buďte A, B množiny. Pravidlo f, které každému prvku $a \in A$ přiřazuje právě jeden prvek $b \in B$, se nazývá **zobrazení množiny** A **do množiny** B. Píšeme $b = f(a)$ nebo $a \mapsto f(b)$. Prvek b se nazývá obraz a v zobrazení f.
Zobrazení f se nazývá **prosté** nebo také **injektivní**, když platí: $a_1, a_2 \in A, a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$ (nebo ekvivalentně: $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$).
Zobrazení f se nazývá A **na** B nebo také **surjektivní**, když ke každému $b \in B$ existuje $a \in A$ tak, že $b = f(a)$.
Je-li f prosté zobrazení A na B, nazývá se **bijekce** nebo také **jednojednoznačná korespondence mezi** A **a** B. Bijekce A na A se nazývá **permutace množiny** A.

__Zápisy:__
$f : A \to B$ ... zobrazení f z A do B.
$f : A \rightarrowtail B$ ... prosté zobrazení f z A do B.

$f : A \twoheadrightarrow B$ ... zobrazení f z A na B.
$f : A \rightarrowtail\!\!\!\!\twoheadrightarrow B$ ... bijekce f z A na B.

Dvě zobrazení $f : A \to B$ a $g : C \to D$ jsou stejná právě když $A = C$, $B = D$ a $f(x) = g(x)$ pro každé $x \in A$.

<u>DEFINICE</u> 1.5. Je-li $f : A \to B, C \subseteq A, D \subseteq B$, pak definujeme:
$f(C) := \{f(a) \mid a \in C\}$ ... **obraz** množiny C v zobrazení f.
$f|_C : C \to B$ definované vztahem $f|_C(c) := f(c)$ pro každé $c \in C$ nazýváme **restrikcí zobrazení** f **na množinu** C.
$f^{-1}(D) := \{a \mid a \in A : f(a) \in D\}$ ... **úplný vzor** množiny D v zobrazení f.
Je-li f bijekce A na B, pak $f^{-1}(\{f(a)\}) = \{a\}$ pro každé $a \in A$ a $f(f^{-1}(\{b\})) = \{b\}$ pro každé $b \in B$.
V takovém případě píšeme zjednodušeně $f^{-1}(f(a)) = a$ a $f(f^{-1}(b)) = b$ a takto získané (bijektivní) zobrazení $f^{-1} : B \rightarrowtail\!\!\!\!\twoheadrightarrow A$ nazýváme **inverzní zobrazení k** f. Zřejmě platí: $f^{-1}(b) = a \Leftrightarrow b = f(a)$.
Zobrazení $I_A : A \to A$ definované vztahem $I_A(a) := a$ pro každé $a \in A$ je zřejmě bijekce. Nazývá se **identické zobrazení na** A.
Je-li $B \subseteq A$, pak zobrazení $1_B : A \to \{0, 1\}$ definované vztahem
$1_B(a) := \begin{cases} 1 & \text{pro } a \in B \\ 0 & \text{pro } a \notin B \end{cases}$ nazýváme **charakteristickou funkcí** podmnožiny B (v množině A).

<u>DEFINICE</u> 1.6. Zobrazení $f : I \to A$, kde $I \subseteq \mathbb{Z}$, nazýváme **posloupností prvků z** A a zapisujeme jej ve tvaru $\{a_n\}_{n\in I}$, kde $a_n := f(n)$. Pokud $I = \mathbb{N}$, resp. $I = \mathbb{Z}$, píšeme také $\{a_n\}_{n=1}^{\infty}$, resp. $\{a_n\}_{n=-\infty}^{\infty}$.

<u>DEFINICE</u> 1.7. Nechť $f : A \to B$ a $g : B \to C$ jsou dvě zobrazení, pak zobrazení $h : A \to C$ definované vztahem $h(a) := g(f(a))$ pro každé $a \in A$, nazýváme **složením zobrazení** f **a** g a píšeme $h = gf$.

<u>PŘÍKLAD</u> 1.8. Uvažujme funkční předpis $f(x) := x^2$, pak
$f : \mathbb{R} \to \mathbb{R}$ není ani prosté ani surjektivní,

$f : \mathbb{R} \to \mathbb{R}^+$ je surjektivní, ale není prosté,
$f : \mathbb{R}^+ \to \mathbb{R}^+$ je prosté i surjektivní, tj. je bijekcí.

MNOŽINOVÉ OPERACE
Nechť dále A_i, $i \in I$ značí nějaký systém množin indexovaný prvky i z indexové množiny I.

DEFINICE 1.9 (Sjednocení množin).

$$\begin{aligned} A \cup B &:= \{x \mid (x \in A) \vee (x \in B)\} \\ A \cup B \cup C &:= \{x \mid (x \in A) \vee (x \in B) \vee (x \in C)\} \\ A_1 \cup A_2 \cup \dots \cup A_n &:= \{x \mid \exists i \in \{1, 2, \dots, n\} : x \in A_i\} \\ &\vdots \\ \bigcup_{i \in I} A_i &:= \{x \mid \exists i \in I : x \in A_i\} \end{aligned}$$

DEFINICE 1.10 (Průnik množin).

$$\begin{aligned} A \cap B &:= \{x \mid (x \in A) \wedge (x \in B)\} \\ A \cap B \cap C &:= \{x \mid (x \in A) \wedge (x \in B) \wedge (x \in C)\} \\ A_1 \cap A_2 \cap \dots \cap A_n &:= \{x \mid \forall i \in \{1, 2, \dots, n\} : x \in A_i\} \\ &\vdots \\ \bigcap_{i \in I} A_i &:= \{x \mid \forall i \in I : x \in A_i\} \end{aligned}$$

Jestliže $A \cap B = \emptyset$, říkáme, že množiny A a B jsou **disjunktní**.

DEFINICE 1.11 (Rozdíl množin).

$$A - B := \{x \mid (x \in A) \wedge (x \notin B)\}$$

Příklad:
$\mathbb{R} - \mathbb{Q}$ (resp. šířeji $\mathbb{C} - \mathbb{Q}$) ... množina všech **iracionálních** čísel.

<u>DEFINICE</u> 1.12 (Doplněk (komplement) množiny).
Jestliže všechny uvažované množiny jsou podmnožinami jisté pevně zvolené univerzální množiny (prostoru) X, pak množinu $X - A$ nazýváme **doplňkem** nebo také **komplementem** množiny A (v X) a píšeme A' nebo A^c.

<u>DEFINICE</u> 1.13 (Symetrická diference).

$$A \div B := (A - B) \cup (B - A)$$

<u>DEFINICE</u> 1.14 (Kartézský součin množin).

$$\begin{aligned} A \times B &:= \{[a,b] \,|\, (a \in A) \wedge (b \in B)\} \\ A \times B \times C &:= \{[a,b,c] \,|\, (a \in A) \wedge (b \in B) \wedge (c \in C)\} \\ A_1 \times A_2 \times \cdots \times A_n &:= \{[a_1, a_2, \ldots, a_n] \,|\, \forall\, i \in \{1,2,\ldots,n\} : a_i \in A_i\} \\ &\vdots \end{aligned}$$

$$\prod_{i \in I} A_i := \mathop{\mathsf{X}}_{i \in I} A_i := \{\varphi \,|\, \varphi : I \to \bigcup_{i \in I} A_i, \text{ kde } \varphi(i) \in A_i \,\forall\, i \in I\},$$

kde $[a,b]$, $[a,b,c]$,…,$[a_1, a_2, \ldots, a_n]$ značí uspořádané dvojice, trojice atd. až n-tice: i-tou složku uspořádané n-tice lze považovat za obraz čísla $i \in \{1,2,\ldots,n\}$ v nějakém zobrazení $\varphi : \{1,2,\ldots,n\} \to \bigcup_{i=1}^n A_i$, kde $a_i := \varphi(i) \in A_i$. Odtud pramení zobecnění definice kartézského součinu na libovolný systém množin, kde každá složka koresponduje s indexem $i \in I$ z libovolné indexové množiny I.

Jsou-li všechny množiny v kartézském součinu identické, pak značí:
$A^2 := A \times A$ (kartézský čtverec množiny A),
$A^3 := A \times A \times A, \ldots, A^n := \underbrace{A \times A \times \cdots \times A}_{n\times}$ a obecně $A^I := \mathop{\mathsf{X}}_{i \in I} A$.
Zejména tedy $A^I := \{\varphi \,|\, \varphi : I \to A\}$ označuje množinu všech zobrazeni I do A.

PŘÍKLAD **1.15.**

(1) Nechť $A := \{a, b, c, d\}$ a $B := \{c, d, e, f\}$, pak $A \cup B = \{a, b, c, d, e, f\}$, $A \cap B = \{c, d\}$, $A - B = \{a, b\}$, $B - A = \{e, f\}$ a $A \div B = \{a, b, e, f\}$.

(2) $\mathbb{R}^2$ ... koresponduje s množinou všech bodů roviny,
$\mathbb{R}^3$ ... s množinou všech bodů 3-rozměrného prostoru,
$\mathbb{R}^n$ ... s množinou všech bodů n-rozměrného prostoru a
$\mathbb{R}^{\mathbb{N}}$, resp. $\mathbb{R}^{\mathbb{Z}}$ s množinou všech posloupností reálných čísel.

MNOŽINOVÉ IDENTITY

VĚTA **1.16.**

(1) *Komutativita:* $A \cup B = B \cup A$
(2) *Asociativita:* $(A \cup B) \cup C = A \cup (B \cup C) = A \cup B \cup C$
(3) *Obecná asociativita a komutativita: Všechna možná sjednocení vytvořená všemi možnými uzávorkováními posloupnosti množin* $A_1, A_2, \ldots, A_n$ *v libovolném pořadí jsou rovna jedinému prvku* $A_1 \cup A_2 \cup \cdots \cup A_n$.
(4) $A \cup A = A$, $A \cup \emptyset = A$
(5) $A \subseteq B \Rightarrow A \cup C \subseteq B \cup C$ *pro libovolné* C
(6) $A \subseteq A \cup B$ *pro libovolné* B
(7) $A \cup B = B \Leftrightarrow A \subseteq B$

Důkaz. CVIČENÍ □

VĚTA **1.17.**

(1) *Komutativita:* $A \cap B = B \cap A$
(2) *Asociativita:* $(A \cap B) \cap C = A \cap (B \cap C) = A \cap B \cap C$
(3) *Obecná asociativita a komutativita: Všechny možné průniky vytvořené všemi možnými uzávorkováními posloupnosti množin* $A_1, A_2, \ldots, A_n$ *v libovolném pořadí jsou rovny jedinému prvku* $A_1 \cap A_2 \cap \cdots \cap A_n$.
(4) $A \cap A = A$, $A \cap \emptyset = \emptyset$
(5) $A \subseteq B \Rightarrow A \cap C \subseteq B \cap C$ *pro libovolné* C

(6) $A \cap B \subseteq A$ *pro libovolné* B
(7) $A \cap B = A \quad \Leftrightarrow \quad A \subseteq B$

Důkaz. CVIČENÍ $\square$

<u>VĚTA</u> 1.18 (Distributivní zákon)**.**

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A \cap (B - C) = (A \cap B) - (A \cap C)$$

Důkaz. CVIČENÍ $\square$

Věta 1.19 (Obecný distributivní zákon)**.**
Nechť I je indexová množina a J_i jsou indexové množiny pro každé $i \in I$. Nechť ke každé uspořádané dvojici indexů $[i,j]$, $i \in I, j \in J_i$, je přiřazena množina A_{ij}. Pak platí:

$$\bigcap_{i\in I} \bigcup_{j\in J_i} A_{ij} = \bigcup_{\gamma\in K} \bigcap_{i\in I} A_{i\gamma(i)}$$
$$\bigcup_{i\in I} \bigcap_{j\in J_i} A_{ij} = \bigcap_{\gamma\in K} \bigcup_{i\in I} A_{i\gamma(i)},$$

kde $K := \underset{i\in I}{X} J_i$.

<u>*Poznámka*</u> 1.20*.*
Distributivní zákon $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ z věty 1.18 je speciálním případem 1.19 (analogicky po vzájemné záměně operací průniku a sjednocení): Jestliže provedeme přeznačení množin $A_{11} := A$, $A_{21} := B$ a $A_{22} := C$ a zavedeme indexové množiny $I := \{1,2\}$, $J_1 := \{1\}$ a $J_2 := \{1,2\}$, pak $K := J_1 \times J_2 = \{[1,1],[1,2]\}$, takže dostáváme:
$A_{11} \cap (A_{21} \cup A_{22}) = (A_{11} \cap A_{21}) \cup (A_{11} \cap A_{22})$.
Výše uvedený postup můžeme zobecnit do následujícího důsledku věty 1.19. Ten ilustruje skutečnost, že obecný distributivní zákon pro

průniky a sjednocení funguje analogicky jako při roznásobování součinu součtů čísel.

<u>DŮSLEDEK</u> 1.21.

$$(A_1 \cup A_2 \cup A_3 \dots) \cap (B_1 \cup B_2 \cup B_3 \dots) \cap (C_1 \cup C_2 \cup C_3 \dots) \cap \dots = \\ = \bigcup_{[j,k,l,\dots]} (A_j \cap B_k \cap C_l \dots)$$

$$(A_1 \cap A_2 \cap A_3 \dots) \cup (B_1 \cap B_2 \cap B_3 \dots) \cup (C_1 \cap C_2 \cap C_3 \dots) \cup \dots = \\ = \bigcap_{[j,k,l,\dots]} (A_j \cup B_k \cup C_l \dots)$$

<u>PŘÍKLAD</u> 1.22 (CVIČENÍ)**.**
$(A \cup B \cup C) \cap (D \cup E) \cap (F \cup G \cup H) = ?$.

<u>LEMMA</u> 1.23.

$$A - B = A \cap B',$$

kde komplement B uvažujeme v nějaké množině obsahující A i B.

<u>VĚTA</u> 1.24 (DeMorganova pravidla)**.**
Nechť A je množina a $\{A_i\}_{i \in I}$ systém množin. Pak platí:

$$A - \bigcap_{i \in I} A_i = \bigcup_{i \in I} (A - A_i)$$

$$A - \bigcup_{i \in I} A_i = \bigcap_{i \in I} (A - A_i)$$

<u>DŮSLEDEK</u> 1.25. `[KaSk:Věta 1.4 s.15]`

$$(\bigcap_{i \in I} A_i)' = \bigcup_{i \in I} A_i'$$

$$(\bigcup_{i \in I} A_i)' = \bigcap_{i \in I} A_i',$$

kde komplementy uvažujeme v nějaké množině obsahující všechny množiny A_i, $i \in I$, neboli obsahující jejich sjednocení.

VĚTA 1.26 (Vlastnosti symetrické diference).
Platí

(1) *Komutativita:* $A \div B = B \div A$
(2) *Asociativita:* $(A \div B) \div C = A \div (B \div C)$
(3) *Distributivita s průnikem:* $A \cap (B \div C) = (A \cap B) \div (A \cap C)$
(4) $A \div A = \emptyset$, $A \div \emptyset = \emptyset \div A = A$

DEFINICE 1.27. Nechť $\{A_n\}_{n=1}^{\infty}$ je posloupnost množin. Pak definujeme: $\limsup A_n$ (**limes superior**) jako množinu všech prvků, které leží v nekonečně mnoha množinách A_n a $\liminf A_n$ (**limes inferior**) jako množinu všech prvků, které leží ve skoro všech množinách A_n (tj. ve všech s výjimkou konečného počtu). Zřejmě platí $\liminf A_n \subseteq \limsup A_n$.
Platí-li $\liminf A_n = \limsup A_n =: A$, pravíme, že posloupnost množin $\{A_n\}_{n=1}^{\infty}$ je **konvergentní** a píšeme $A = \lim A_n$.

VĚTA 1.28.
Platí

$$\liminf A_n = \bigcup_{k=1}^{\infty} \bigcap_{n=k}^{\infty} A_n$$
$$\limsup A_n = \bigcap_{k=1}^{\infty} \bigcup_{n=k}^{\infty} A_n$$

<u>DŮKAZ</u>. $x \in \limsup A_n \Leftrightarrow x$ leží v nekonečně mnoha množinách $A_n \Leftrightarrow x \in \bigcup_{n=k}^{\infty}$ pro každé $k = 1, 2, \ldots \Leftrightarrow x \in \bigcap_{k=1}^{\infty} \bigcup_{n=k}^{\infty} A_n$.
Druhá identita se dokáže analogicky (cvičení). □

DŮSLEDEK 1.29. *Monotonní posloupnost je konvergentní. Přitom*

(1) *je-li posloupnost neklesající:* $A_1 \subseteq A_2 \subseteq A_3 \subseteq \ldots$, *pak* $\lim A_n = \bigcup_{n=1}^{\infty} A_n =: A$ *a píšeme* $A_n \uparrow A$.
(2) *je-li posloupnost nerostoucí:* $A_1 \supseteq A_2 \supseteq A_3 \supseteq \ldots$, *pak* $\lim A_n = \bigcap_{n=1}^{\infty} A_n =: A$ *a píšeme* $A_n \downarrow A$.

MOHUTNOSTI MNOŽIN A KARDINÁLNÍ ČÍSLA

DEFINICE 1.30. Množiny A a B se nazývají **ekvivalentní**, píšeme $A \sim B$, jestliže existuje bijekce A na B. Říkáme také, že A a B mají **stejnou mohutnost** a píšeme $\operatorname{card} A = \operatorname{card} B$. Symbol $a := \operatorname{card} A$ pak nazýváme **mohutností** nebo **kardinálním číslem** množiny A. Jestliže existuje injekce A do B (neboli A je ekvivalentní s nějakou podmnožinou B), píšeme $\operatorname{card} A \leq \operatorname{card} B$. Pokud přitom A a B nemají stejnou mohutnost, tj. $\operatorname{card} A \neq \operatorname{card} B$, píšeme $\operatorname{card} A < \operatorname{card} B$.

DEFINICE 1.31. Každá množina ekvivalentní s množinou všech přirozených čísel $\mathbb{N}$ se nazývá **spočetná**.

DEFINICE 1.32. Nekonečná množina, která není spočetná se nazývá **nespočetná**.

VĚTA 1.33 (viz také dále 1.34 a 1.35).
Interval $[0, 1]$ *je nespočetný.*

DEFINICE 1.34. Říkáme, že množina M je množina **o mohutnosti kontinua**, je-li $M \sim [0, 1]$.

VĚTA 1.35 (viz také dále 1.59(2)).
Každý netriviální interval (tj. interval obsahující více jak jeden prvek) má mohutnost kontinua.

Poznámka 1.36.
(1) Pro množiny, které nejsou nekonečné, udává mohutnost počet jejich prvků:

$\operatorname{card} \emptyset =: 0$

$\operatorname{card} \{a_1, a_2, \dots, a_n\} =: n$

(2) Pro zápis mohutnosti nekonečných množin je používán symbol $\aleph$ (čteme *alef*: písmeno A hebrejské abecedy):

A spočetná: $\operatorname{card} A =: \aleph_0$

A o mohutnosti kontinua: $\operatorname{card} A =: \aleph$.

(3) Pro zápis mohutnosti disjunktního sjednocení množin je používán symbol $+$ nebo $\sum$:

$\operatorname{card}(\bigcup_{i\in I} A_i) =: \sum_{i\in I} \operatorname{card} A_i$
$\operatorname{card}(A_1 \cup A_2 \cup \dots \cup A_n) =: \operatorname{card} A_1 + \operatorname{card} A_1 + \dots + \operatorname{card} A_n$.

(4) Pro zápis mohutnosti kartézského součinu množin je používán symbol $\cdot$ nebo $\prod$:

$\operatorname{card}(\underset{i\in I}{\mathsf{X}} A_i) =: \prod_{i\in I} \operatorname{card} A_i$, resp. $\operatorname{card}(A^I) =: (\operatorname{card} A)^{\operatorname{card} I}$,

Speciálně $\operatorname{card}(A^\emptyset) =: (\operatorname{card} A)^0 =: 1$, tj. množina všech zobrazení z prázdné množiny do A se považuje za jednoprvkovou množinu obsahující tzv. **prázdné zobrazení**.

$\operatorname{card}(A_1 \times A_2 \times \dots \times A_n) =: \operatorname{card} A_1 \cdot \operatorname{card} A_1 \cdots \operatorname{card} A_n$, resp.
$\operatorname{card}(A^n) =: (\operatorname{card} A)^n$.

VĚTA 1.37.
Buď I indexová množina a $\{A_i\}_{i\in I}$ a $\{B_i\}_{i\in I}$ dva systémy množin takové, že $A_i \sim B_i$ pro každé $i \in I$. Pak platí:

(1) $\underset{i\in I}{\mathsf{X}} A_i \sim \underset{i\in I}{\mathsf{X}} B_i$
(2) *Jsou-li množiny A_i po dvou disjunktní a rovněž množiny B_i po dvou disjunktní, platí také $\bigcup_{i\in I} A_i \sim \bigcup_{i\in I} B_i$.*

DŮSLEDEK 1.38. $A_1 \sim B_1, A_2 \sim B_2 \Rightarrow A_1 \times A_2 \sim B_1 \times B_2$. *Jsou-li navíc jak A_1, A_2 tak B_1, B_2 disjunktní, platí navíc $A_1 \cup A_2 \sim B_1 \cup B_2$.*

VĚTA 1.39.
Buď dán systém množin $\{A_i\}_{i\in I}$, kde množiny A_i jsou po dvou disjunktní a $A_i \sim A$ pro každé $i \in I$.
Pak $\bigcup_{i\in I} A_i \sim I \times A$ a $\sum_{i\in I}(\operatorname{card} A_i) = \operatorname{card} I \cdot \operatorname{card} A$.

VĚTA 1.40 (`[KaSk:V4.6 s.39]`,)**.**
Nechť $A_2 \subseteq A_1 \subseteq A$ a nechť $A_2 \sim A$. Pak také $A_1 \sim A$. Neboli $\operatorname{card} A_2 \le \operatorname{card} A_1 \le \operatorname{card} A \Rightarrow \operatorname{card} A_1 = \operatorname{card} A$.

DŮSLEDEK 1.41. *Nechť A, B jsou dvě množiny, z nichž každá je ekvivalentní s podmnožinou druhé. Pak $A \sim B$. Zejména tedy platí:* $(\operatorname{card} A \le \operatorname{card} B) \wedge (\operatorname{card} B \le \operatorname{card} A) \Leftrightarrow (\operatorname{card} A = \operatorname{card} B)$.

Zejména tedy pro žádné dvě množiny A a B nemůže současně platit $\operatorname{card} A < \operatorname{card} B$ *a* $\operatorname{card} B < \operatorname{card} A$.

Věta 1.42 (Komut. zákon pro kartézský součin). *Nechť je dán systém množin $\{A_i\}_{i\in I}$, $a_i := \operatorname{card} A_i$, a $I \sim J$, kde f je bijekce J na I. Pak $\underset{i\in I}{X} A_i \sim \underset{j\in J}{X} A_{f(j)}$ a $\prod_{i\in I} a_i = \prod_{j\in J} a_{f(j)}$.*

DŮSLEDEK 1.43.

(1) *Je-li f permutace množiny I, pak platí $\underset{i\in I}{X} A_i \sim \underset{i\in I}{X} A_{f(i)}$ a $\prod_{i\in I} a_i = \prod_{i\in I} a_{f(i)}$.*

(2) $A \times B \sim B \times A$ *a* $\operatorname{card} A \cdot \operatorname{card} B = \operatorname{card} B \cdot \operatorname{card} A$.

Věta 1.44 (Asoc. zákon pro kartézský součin). *Nechť je dán systém množin $\{A_i\}_{i\in I}$, $a_i := \operatorname{card} A_i$, a $I = \bigcup_{k\in K} I_k$, kde množiny I_k jsou po dvou disjunktní. Pak platí $\underset{i\in I}{X} A_i \sim \underset{k\in K}{X}(\underset{i\in I_k}{X} A_i)$, $\prod_{i\in I} a_i = \prod_{k\in K}(\prod_{i\in I_k} a_i)$.*

DŮSLEDEK 1.45.

(1) *Platí $A \times (B \times C) \sim (A \times B) \times C \sim A \times B \times C$, $a\cdot(b\cdot c) = (a\cdot b)\cdot c = a\cdot b\cdot c$, kde a, b, c značí po řadě mohutnosti množin A, B, C.*

(2) *Nechť $I = \bigcup_{k\in K} I_k$, kde I_k jsou po dvou disjunktní. Pak platí $A^I \sim \underset{k\in K}{X} A^{I_k}$ a*
$(\operatorname{card} A)^{\sum_{k\in K} \operatorname{card} I_k} = \prod_{k\in K} (\operatorname{card} A)^{\operatorname{card} I_k}$. *Zejména*
$A^{I_1 \cup I_2} \sim A^{I_1} \times A^{I_2}$ *a*
$\operatorname{card} A^{\operatorname{card} I_1 + \operatorname{card} I_2} = \operatorname{card} A^{\operatorname{card} I_1} \cdot \operatorname{card} A^{\operatorname{card} I_2}$,
jsou-li I_1 a I_2 disjunktní.

(3) *Nechť M je množina, $m := \operatorname{card} M$, a nechť je dán systém množin $\{A_i\}_{i\in I}$, $a_i := \operatorname{card} A_i$. Pak platí*
$(\underset{i\in I}{X} A_i)^M \sim \underset{i\in I}{X} A_i^M$, $(\prod_{i\in I} a_i)^m = \prod_{i\in I} a_i^m$.
Zejména $(A \times B)^M \sim A^M \times B^M$, $(a \cdot b)^m = a^m \cdot b^m$, kde a, b jsou po řadě mohutnosti množin A, B.

(4) *Pro libovolné množiny* A, M, N *a jejich mohutnosti* a, m, n *platí* $A^{M\times N} \sim (A^M)^N$, $a^{m\cdot n} = a^m \cdot a^n$.

Věta 1.46 (Distr. zákony pro kartézský součin). *Nechť* I *je indexová množina a* J_i *jsou indexové množiny pro každé* $i \in I$. *Nechť ke každé uspořádané dvojici indexů* $[i, j]$ *je přiřazena množina* A_{ij}. *Pak platí:*

$$\mathop{\mathsf{X}}_{i\in I} \bigcup_{j\in J_i} A_{ij} = \bigcup_{\gamma\in K} \mathop{\mathsf{X}}_{i\in I} A_{i\gamma(i)}$$

$$\mathop{\mathsf{X}}_{i\in I} \bigcap_{j\in J_i} A_{ij} = \bigcap_{\gamma\in K} \mathop{\mathsf{X}}_{i\in I} A_{i\gamma(i)}$$

kde $K := \mathop{\mathsf{X}}_{i\in I} J_i$.

DŮSLEDEK 1.47.
Platí

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$
$$A \times (B \cap C) = (A \times B) \cap (A \times C)$$

VĚTA 1.48.
Buď M *množina a* B *množina obsahující dva prvky. Označme* $\mathcal{P}(M)$ *množinu všech podmnožin množiny* M *(někdy se také značí poněkud nepřesně jako* 2^M*). Pak* $\mathcal{P}(M) \sim B^M$ *a* $\mathrm{card}\,(\mathcal{P}(M)) = 2^{\mathrm{card}\, M}$.

VĚTA 1.49 (Cantorova věta `[KaSk:V4.14-15 s.41]`).
Pro každé kardinální číslo a platí $2^a > a$.

VĚTA 1.50.
Množina A *je spočetná tehdy a jen tehdy, když její prvky lze očíslovat přirozenými čísly, tj. když ji lze psát ve tvaru posloupnosti:* $A := \{a_1, a_2, \dots, a_n, \dots\} = \{a_n\}_{n=1}^{\infty}$.

PŘÍKLAD 1.51.
Příklady spočetných množin:

- $\mathbb{N} := \{1, 2, 3, \dots, n, \dots\}$ … množina přirozených čísel
- $\{2, 4, 6, \dots, 2n, \dots\}$ … množina sudých přirozených čísel

- $\{1, 3, 5, \dots, 2n-1, \dots\}$ ... množina lichých přirozených čísel
- $\{1, 4, 9, \dots, n^2, \dots\}$ ... množina kvadrátů přirozených čísel
- $\{1, \frac{1}{2}, \frac{1}{3}, \dots, \frac{1}{n}, \dots\}$ ... množina převrácených hodnot přirozených čísel

<u>VĚTA</u> 1.52 (Vlastnosti spočetných množin)**.**

(1) *Každá nekonečná množina obsahuje (vlastní) spočetnou podmnožinu.*
(2) *Každá nekonečná podmnožina spočetné množiny je spočetná.*
(3) *Rozdíl spočetné množiny a konečné množiny je spočetná množina ($\aleph_0 - n = \aleph_0$ pro každé $n \in \mathbb{N}$).*
(4) *Sjednocení spočetné množiny a konečné množiny je spočetná množina ($\aleph_0 + n = \aleph_0$ pro každé $n \in \mathbb{N}$).*
(5) *Sjednocení konečného počtu spočetných množin je spočetná množina ($n \cdot \aleph_0 = \aleph_0$ pro každé $n \in \mathbb{N}$).*
(6) *Sjednocení spočetné množiny neprázdných po dvou disjunktních konečných množin je spočetná množina ($\aleph_0 \cdot n = \aleph_0$ pro každé $n \in \mathbb{N}$).*
(7) *Kartézský součin konečného počtu spočetných množin je spočetná množina ($\aleph_0^n = \aleph_0$ pro každé $n \in \mathbb{N}$).*

Důkaz. . □

<u>DŮSLEDEK</u> 1.53.

(1) *Sjednocení spočetné množiny spočetných množin je spočetná množina.*
(2) *Množina všech celých i racionálních čísel je spočetná.*
(3) *Množina všech racionálních čísel netriviálního intervalu reálných čísel je spočetná.*
(4) *Množina všech bodů v rovině (v prostoru) s racionálními souřadnicemi je spočetná.*
(5) *Množina všech komplexních čísel s racionální reálnou i imaginární částí je spočetná.*

(6) *Množina všech polynomů s celými (racionálními) koeficienty je spočetná.*
(7) *Množina všech algebraických čísel je spočetná (***algebraickým číslem** *rozumíme reálné číslo, které je kořenem nějakého polynomu s celočíselnými koeficienty).*

<u>VĚTA</u> 1.54.
Je-li M nekonečná a A nejvýše spočetná množina (tj. konečná nebo spočetná), pak $M \cup A \sim M$ (neboli $M \cup A$ má stejnou mohutnost jako M).

<u>DŮSLEDEK</u> 1.55.
Nechť M je spočetná množina, pak $\mathcal{P}(M)$ má mohutnost kontinua a platí $2^{\aleph_0} = \aleph > \aleph_0$.

<u>VĚTA</u> 1.56.
Buď M nespočetná množina a A její nejvýše spočetná podmnožina. Pak $M - A \sim M$. Je-li A konečná, platí tvrzení i pro spočetnou množinu M dle 1.52(3).

<u>DŮSLEDEK</u> 1.57. *Množina M je nekonečná právě když obsahuje vlastní podmnožinu stejné mohutnosti jako M.*

<u>VĚTA</u> 1.58 (Vlastnosti množin o mohutnosti kontinua)**.**
(1) *Každá množina o mohutnosti kontinua obsahuje vlastní podmnožinu o mohutnosti kontinua [plyne z 1.57].*
(2) *Rozdíl množiny o mohutnosti kontinua a nejvýše spočetné množiny má mohutnost kontinua ($\aleph - n = \aleph - \aleph_0 = \aleph$ pro každé $n \in \mathbb{N}$) [plyne z 1.56].*
(3) *Sjednocení množiny o mohutnosti kontinua a nejvýše spočetné množiny je množina o mohutnosti kontinua ($\aleph + n = \aleph + \aleph_0 = \aleph$ pro každé $n \in \mathbb{N}$) [plyne z 1.54].*
(4) *Sjednocení nejvýše spočetné množiny po dvou disjunktních množin o mohutnosti kontinua má mohutnost kontinua ($n \cdot \aleph = \aleph_0 \cdot \aleph = \aleph$ pro každé $n \in \mathbb{N}$) .*

(5) *Kartézský součin spočetně mnoha dvouprvkových množin má mohutnost kontinua ($\aleph = 2^{\aleph_0} > \aleph_0$) [plyne z 1.55 a z 1.48].*
(6) *Množina všech posloupností přirozených čísel má mohutnost kontinua ($\aleph_0^{\aleph_0} = \aleph$) .*
(7) *Kartézský součin nejvýše spočetně mnoha množin o mohutnosti kontinua má mohutnost kontinua ($\aleph^n = \aleph^{\aleph_0} = \aleph$ pro každé $n \in \mathbb{N}$) .*

<u>DŮSLEDEK</u> 1.59.

(1) *Sjednocení nejvýše spočetné množiny množin o mohutnosti kontinua má mohutnost kontinua [plyne z 1.58(4) užitím 1.40].*
(2) *Každý netriviální interval i jeho nejvýše spočetná mocnina mají mohutnost kontinua [viz 1.54, 1.56 a 1.58(4)(7)]. Zejména $\mathbb{R}^n$ pro každé $n \in \mathbb{N}$ i $\mathbb{R}^{\mathbb{N}}$ mají mohutnost kontinua.*
(3) *Množina všech iracionálních čísel má mohutnost kontinua [plyne ze (2) a z 1.58(2)] .*
(4) *Množina všech transcendentních čísel má mohutnost kontinua (***transcendentním číslem** *nazýváme každé reálné číslo, které není algebraické) [plyne ze 1.53(7) a z 1.58(2)].*
(5) *Množina všech bodů v rovině má mohutnost kontinua [plyne ze (2)]. Zejména $\mathbb{C}$ má také mohutnost kontinua.*
(6) *Buď dán systém množin $\{A_i\}_{i \in I}$, kde množiny A_i jsou po dvou disjunktní a každá z nich má mohutnost kontinua stejně jako indexová množina I. Pak $\bigcup_{i \in I} A_i$ má rovněž mohutnost kontinua [plyne z 1.58(7) spolu s 1.39].*
(7) *Kartézský součin spočetně mnoha nejvýše spočetných množin o alespoň dvou prvcích má mohutnost kontinua ($n^{\aleph_0} = \aleph_0^{\aleph_0} = \aleph$ pro každé $n \in \mathbb{N}$, $n \geq 2$) [plyne z 1.58(5)(6) užitím 1.40].*

1.3. **Číselné obory.**
V této kapitole shrneme základní poznatky o číselných oborech, které se nejčastěji vyskytují v matematice.

MNOŽINA PŘIROZENÝCH ČÍSEL $\mathbb{N}$
$\mathbb{N} := \{1, 2, \dots, n, \dots\}$.
Operace: sečítání $+$, násobení $.$ a z něj odvozené umocňování:
$n^k := \underbrace{n \times n \times \cdots \times n}_{k\times}$, $k \in \mathbb{N}$, $n^0 := 1$.
Význačné prvky: jednotkový prvek 1 ($1.n = n.1 = n \ \forall n \in \mathbb{N}$)
Mohutnost: $\operatorname{card} \mathbb{N} = \aleph_0$ dle 1.31 a 1.36(2).

MNOŽINA CELÝCH ČÍSEL $\mathbb{Z}$
Příklady: `[Ho:neřešené §3; s.45-47]`
$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots, n, \dots\} = \{-n \,|\, n \in \mathbb{N}\} \cup \{0\} \cup \mathbb{N}$.
Operace: sečítání $+$, odečítání $-$, násobení $.$ a z něj odvozené umocňování: $n^k := \underbrace{n \times n \times \cdots \times n}_{k\times}$, $k \in \mathbb{N}$, $n^0 := 1$ pro $n \neq 0$.
Význačné prvky:
- jednotkový prvek 1 ($1.n = n.1 = n \ \forall n \in \mathbb{Z}$)
- nulový prvek 0 ($0 + n = n + 0 = n \ \forall n \in \mathbb{Z}$)

Mohutnost: $\operatorname{card} \mathbb{Z} = \aleph_0$ dle 1.53(2).

MNOŽINA CELÝCH ČÍSEL MODULO N: $\mathbb{Z}_N$
$\mathbb{Z}_N := \{0, 1, \dots, N-1\}$ pro každé $N \in \mathbb{N}$.
Jelikož každé celé číslo $n \in \mathbb{Z}$ lze jednoznačně vyjádřit ve tvaru $n = q.N + r$ (q je celá část podílu a $r \in \mathbb{Z}_N$ zbytek po dělení), můžeme zavést surjektivní zobrazení $\langle\cdot\rangle_N : \mathbb{Z} \twoheadrightarrow \mathbb{Z}_N$ přiřazující každému celému číslu n jeho zbytek po dělení číslem N: tzv. **operace modulo**. Pomocí této operace zavedeme tzv. **modulární aritmetiku** na $\mathbb{Z}_N$.
Operace:
- sečítání modulo N: $a \oplus b := a + b \mod N := \langle a + b\rangle_N$,
- odečítání modulo N: $a \ominus b := a - b \mod N := \langle a - b\rangle_N$,
- násobení modulo N: $a \odot b := a.b \mod N := \langle a.b\rangle_N$

a z něj odvozené umocňování modulo N:
$n^k \mod N := \langle n^k\rangle_N$, $k\in\mathbb{N}$, $n^0 \mod N := 1$ pro $n\neq 0$.
Význačné prvky:
• jednotkový prvek 1 při $N>1$ ($1\odot n = n\odot 1 = n\ \forall n\in\mathbb{Z}_N$)
• nulový prvek 0 ($0\oplus n = n\oplus 0 = n\ \forall n\in\mathbb{Z}_N$)
Mohutnost: $\operatorname{card}\mathbb{Z}_N = N$ dle 1.36(1).

MNOŽINA RACIONÁLNÍCH ČÍSEL $\mathbb{Q}$
$\mathbb{Q} := \{\frac{p}{q}\mid \frac{p}{q}$ je hodnota zlomku s čit. p a jmenov. q, $p,q\in\mathbb{Z}, q\neq 0\}$.
Je-li $q=1$, pak $\frac{p}{q}=p$ a tedy $\mathbb{Z}\subset\mathbb{Q}$.
Operace: sečítání $+$, odečítání $-$, dělení nenulovým číslem $/$, násobení . a z něj odvozené umocňování:
$r^k := \underbrace{r\times r\times\cdots\times r}_{k\times}$, $k\in\mathbb{N}$;
pro $r\neq 0$ definujeme $r^0:=1$ a $r^{-k}:=(1/r)^k$.
Význačné prvky:
• jednotkový prvek 1 ($1.r = r.1 = r\ \forall r\in\mathbb{Q}$)
• nulový prvek 0 ($0+r = r+0 = r\ \forall r\in\mathbb{Q}$)
Mohutnost: $\operatorname{card}\mathbb{Q} = \aleph_0$ dle 1.53(2).

MNOŽINA REÁLNÝCH ČÍSEL $\mathbb{R}$
$\mathbb{R} := \{r\mid r = d_k\,d_{k-1}\,\ldots\,d_0, d_{-1}\,d_{-2}\,\ldots$ je desetinné vyjádření čísla r$\}$.
Tedy $r=\sum_{j=-\infty}^{k} d_j 10^j$, $k\in\mathbb{Z}$, $k\geq 0$, kde $d_j\in\mathbb{Z}_{10}$, jsou dekadické cifry vyjádření čísla r v soustavě o základu 10, tj. pro $k\in\mathbb{N}$ je d_{k-1} k-tá cifra před desetinnou čárkou a d_{-k} k-tá cifra za desetinnou čárkou.
Každé reálné číslo lze vyjádřit v libovolné soustavě o základu $N\in\mathbb{N}$, $N\geq 2$, kdy $r=\sum_{j=-\infty}^{k} d_j N^j$, $k\in\mathbb{Z}$, $k\geq 0$, kde $d_j\in\mathbb{Z}_N$.
V paměti počítačů se užívají soustavy o základu $N=2$ (**dvojková, binární, dyadická**), kde cifry $d_j\in\{0,1\}$; $N=8$ (**osmičková, oktalová**) nebo $N=16$ (**šestnáctková, hexadecimální**), kde cifry $d_j\geq 10$ obvykle nahrazujeme písmeny: $10 =: A, 11 =: B, 12 =: C, 13 =: D, 14 =: E, 15 =: F$.

Množina $\mathbb{R}$ představuje **zúplnění** množiny $\mathbb{Q}$ v tom smyslu, že každé reálné číslo je 'limitou' nějaké posloupnosti racionálních čísel. Například stačí vzít useknuté desetinné rozvoje
$\sum_{j=-m}^{k} d_j 10^j = d_k\, d_{k-1} \dots d_0, d_{-1}\, d_{-2} \dots d_{-m}$ postupně s $m = 1, 2, \dots$ místy za desetinnou čárkou, které představují racionální čísla blížící se pro $m \to \infty$ k číslu r.
Operace: sečítání $+$, odečítání $-$, dělení nenulovým číslem $/$, násobení . a z něj odvozené umocňování
$r^k := \underbrace{r \times r \times \cdots \times r}_{k\times}$, kde $r \in \mathbb{R}$ a $k \in \mathbb{N}$;
pro $r \neq 0$ definujeme $r^0 := 1$ a $r^{-k} := (1/r)^k$.
Pokud $r > 0$, lze umocňování dále rozšířit na r^s i pro reálný exponent $s \in \mathbb{R}$, přičemž platí $r^{-s} := (1/r)^s$.
Význačné prvky:
• jednotkový prvek 1 ($1.r = r.1 = r\ \forall r \in \mathbb{R}$)
• nulový prvek 0 ($0 + r = r + 0 = r\ \forall r \in \mathbb{R}$)
Mohutnost: $\operatorname{card} \mathbb{R} = \aleph$ dle 1.59(2).

MNOŽINA IRACIONÁLNÍCH ČÍSEL $\mathbb{I}$
$\mathbb{I} := \mathbb{R} - \mathbb{Q}$.
Mohutnost: $\operatorname{card} \mathbb{I} = \aleph$ dle 1.59(3).

MNOŽINA ALGEBRAICKÝCH ČÍSEL $\mathbb{A}$
Dle 1.53(7) algebraickým číslem rozumíme každé reálné číslo $a \in \mathbb{R}$, které je kořenem nějakého polynomu s celočíselnými koeficienty, tj. platí $P(a) = 0$, pro nějaký polynom $P(x) = p_0 + p_1 x + \cdots + p_n x^n$ stupně $n \in \mathbb{N}$, kde $p_i \in \mathbb{Z}\ \forall\, i \in \mathbb{Z}$, $p_n \neq 0$.
Je $\mathbb{Q} \subset \mathbb{A}$, neboť každé racionální číslo $\frac{p}{q}$, $q \neq 0$, je řešením lineární rovnice $q.x - p = 0$. Existují však další algebraická čísla: například $\sqrt[n]{m}$ pro libovolné $m, n \in \mathbb{N}$, $n > 1$, je řešením rovnice $x^n - m = 0$. Zejména $\sqrt{2}$ je algebraické číslo, které není racionální.
Mohutnost: $\operatorname{card} \mathbb{A} = \aleph_0$ dle 1.53(7).

MNOŽINA TRANSCENDENTNÍCH ČÍSEL $\mathbb{T}$

Dle 1.59(4) definujeme $\mathbb{T} := \mathbb{R} - \mathbb{A} \subset \mathbb{R} - \mathbb{Q} = \mathbb{I}$.
Nejznámějšími příklady transcendentních čísel jsou čísla
$e := 2.718281828459\ldots$ základ tzv. **přirozeného logaritmu** ln a
$\pi := 3.1415926535897\ldots$ **Ludolfovo číslo**=délka kružnice o průměru 1.
Mohutnost: $\operatorname{card} \mathbb{T} = \aleph$ dle 1.59(4).

MNOŽINA KOMPLEXNÍCH ČÍSEL $\mathbb{C}$

Motivací pro zavedení komplexních čísel je skutečnost, že některé polynomické rovnice $P(x) = 0$ s reálnými koeficienty nemají reálný kořen. Například $x^2 + 1 > 0$ pro každé $x \in \mathbb{R}$. Jestliže označíme speciálním symbolem $i := \sqrt{-1}$ nazývaným **imaginární jednotka**, pak $i^2 = -1$ můžeme považovat za řešení odpovídající rovnice $x^2 + 1 = 0$ (někdy místo i se používá symbol j). Zavedeme-li množinu **tzv. komplexních čísel** jako množinu formálních součtů reálných čísel s reálnými násobky imaginární jednotky, tj.
$\mathbb{C} := \{a + i.b \,|\, a \in \mathbb{R},\, b \in \mathbb{R}\}$,
pak se dá ukázat, že uvedený problém bude odstraněn: každý polynom stupně n s komplexními koeficienty bude mít právě n kořenů. To odpovídá zkušenosti z reálného oboru s rovnicí $x^2 - 1$, která má dva kořeny -1 a 1. V rozšířeném oboru komplexních čísel $\mathbb{C}$ pak podobně rovnice $x^2 + 1$ má dva kořeny $-i$ a i.
Značení: Je-li $c = a + i.b$ komplexní číslo, pak značí
$\operatorname{Re} c := a$ ... **reálnou část** c
$\operatorname{Im} c := b$ ... **imaginární část** c
$|c| := \sqrt{a^2 + b^2}$ ... **velikost (absolutní hodnotu, modul)** c
$\alpha := \arctan(\frac{b}{a}), 0 \leq \alpha < 2\pi$ ... **argument** c
$\overline{c} := a - i.b$ ... číslo komplexně sdružené k c (zřejmě $c.\overline{c} = |c|^2$).

Zřejmě $\mathbb{C} \sim \{[a, b] \,|\, a \in \mathbb{R}, b \in \mathbb{R}\} = \mathbb{R}^2$, takže každé komplexní číslo $a + i.b$ můžeme znázornit jako bod v kartézské rovině o souřadnicích a, b. Tato rovina se pak nazývá **komplexní rovina**.

Dostáváme tak tři základní tvary pro vyjádření komplexního čísla:
• **kartézský:** $c = a + i.b$
• **goniometrický:** $c = A(\cos\alpha + i\sin\alpha)$, který odpovídá přechodu k polárním souřadnicím: $a = A\cos\alpha$, $b = A\sin\alpha$.
• **Eulerův:** $c := Ae^{i\alpha}$, kde $e^{i\alpha} := \cos\alpha + i\sin\alpha$ je komplexní číslo na jednotkové kružnici v komplexní rovině.
$\mathbb{R} = \{c \in \mathbb{C} \,|\, \mathrm{Im}\, c = 0\} \subset \mathbb{C}$, přičemž operace z $\mathbb{R}$ rozšíříme formálně na $\mathbb{C}$ za užití vlastnosti $i^2 = -1$ při operacích násobení a dělení. Operace sečítání (odečítání) se provádí po složkách jako s vektory v rovině. Tyto výpočty pak formálně usnadňuje Eulerův zápis.
Odtud dostáváme s uvážením $\frac{1}{i} = \frac{i}{i.i} = -i$:

$$i^0 = 1, i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1, \text{ obecně: } i^{4n+k} = i^k \ \forall n, k \in \mathbb{Z}.$$

Operace (podrobněji viz přílohu A):
sečítání $+$, odečítání $-$, dělení nenulovým číslem $/$, násobení $.$ a z něj odvozené umocňování (resp. odmocňování)
$c^k := \underbrace{c \times c \times \cdots \times c}_{k\times}$, kde $c \in \mathbb{C}$ a $k \in \mathbb{N}$;
pro $c \neq 0$ lze umocňování dále rozšířit na c^s i pro komplexní exponent $s \in \mathbb{C}$, přičemž platí $c^{-s} := (1/c)^s$.
Význačné prvky:
• jednotkový prvek $1 := 1 + i.0$ $(1.c = c.1 = c \ \forall c \in \mathbb{C})$
• nulový prvek $0 := 0 + i.0$ $(0 + c = c + 0 = c \ \forall r \in \mathbb{R})$.
Mohutnost: $\mathrm{card}\,\mathbb{C} = \aleph$ dle 1.59(5).

ANGLICKÁ TERMINOLOGIE TEORIE MNOŽIN

množina, prázdná množina ♦ set, empty set
(vlastní) podmnožina, nadmnožina ♦ (proper) subset, superset
zobrazení, prosté, inverzní ♦ mapping, injective, inverse
surjektivní (na), bijektivní ♦ surjective (onto), bijective
permutace ♦ permutation
obraz, úplný vzor ♦ image, preimage (inverse image)
posloupnost ♦ sequence
sjednocení, průnik ♦ union, intersection
(kartézský) součin, mocnina ♦ (cartesian) product, power
disjunktní, po dvou disjunktní ♦ disjoint, pairwise disjoint
rozdíl, symetrická diference ♦ difference, symmetric difference
monotonní, konvergentní ♦ monotone, convergent
mohutnost, kardinální číslo ♦ cardinality, cardinal number
spočetný, nespočetný ♦ countable, uncountable
mohutnost kontinua ♦ continuum power
konečný, nekonečný ♦ finite, infinite
množina všech podmnožin ♦ power set
číslo, reálné, komplexní♦ mumber, real, complex
celé, racionální, iracionální ♦ integer, rational, irrational
algebraické, transcendentní ♦ algebraic, transcendental
komplexně sdružené číslo ♦ complex conjugate number

MATLAB

`logical` ... transformace čísla na logický typ:
$a \neq 0 \Rightarrow$ `logical(a)=true` (platí), `logical(0)=false` (neplatí)
`mod` ... operace modulo: `mod(n,N)` $= \langle n \rangle_N$.
`i`,`j` ... imaginární jednotka.
Logické operátory: `~A` (negace A), `A & B` (konjunkce), `A | B` (disjunkce), `xor(A,B)`... buď a nebo. Ostatní logické operátory se z nich složí pomocí ekvivalentních logických formulí (viz 1.1).
Zápisy množin:
například {`a1,a2,a3`} nebo `[a1,a2,a3]` ... řádková verze. Jako oddělovač lze užít i středník (sloupcová verze).
Množinové operace:
`ismember(A,B)` ... testuje příslušnost prvků z A v B
`unique(A)` ... odstraní z A duplicitní prvky
`union(A,B)` ... sjednocení množin A a B
`intersect(A,B)` ... průnik množin A a B
`setdiff(A,B)` ... rozdíl množin A a B
`setxor(A,B)` ... symetrická diference množin A a B
Ostatní operace lze vytvořit (simulovat) pomocí vhodných složených výrazů.

2. Algebraické struktury

Teorie a příklady: `[KaSk: s.26-36,44-53]`
Příklady: `[Ho:řešené č.5,6,11-15; s.8,9,13-16]`,
`[Ho:neřešené kap.1,§4-7,kap.2 s.47-80]`

MOTIVACE

V reálném světě se objekty zařazované do množin často vyznačují specifickými vlastnostmi: můžeme je dávat do nejrůznějších souvislostí (relací) – např. je porovnávat, vybírat mezi nimi jisté význačné prvky se specifickou rolí, provádět různé operace, měřit velikost či vzdálenost, nebo u některých podmnožin jejich délku, plochu, objem, hmotnost apod.
Nejnázornějším motivačním příkladem může sloužit v tomto směru množina reálných čísel $\mathbb{R}$. Její prvky lze porovnávat (relace uspořádání), sečítat či násobit, roli význačných prvků hraje 0 a 1, velikost a vzdálenost měříme absolutní hodnotou, intervaly jsou specifické podmnožiny, jimž lze přiřadit délku apod.
Algebraické struktury představují abstraktní konstrukci umožňující přenášet vybrané strukturní vlastnosti reálné přímky i na množiny sice s jinými prvky ale podobného charakteru. Nepřeneseme-li vlastnosti všechny, ale jen některé, část strukturních rysů reálné přímky ztratíme, některé však zůstanou zachovány. Cílem této (ale i následující) kapitoly je podat přehled nejčastěji používaných matematických struktur a jejich základních vlastností.

DEFINICE 2.1. V širším smyslu **(algebraickou) strukturou** rozumíme uspořádanou dvojici $(N, \mathcal{S})$, kde $N \neq \emptyset$ je samotná množina, tzv. **nosič algebraické struktury**, a $\mathcal{S}$ systém množin popisující její strukturu (množina relací, operací, význačných prvků, specifických podmnožin apod.). Jestliže například $\mathcal{S} = \{+, \circ, 1\}$, píšeme také $(N, +, \circ, 1)$ místo $(N, \{+, \circ, 1\})$.

DEFINICE 2.2. Jsou-li $(N_1, \mathcal{S}_1)$ a $(N_2, \mathcal{S}_2)$ dvě algebraické struktury téhož typu[1] a $f : N_1 \to N_2$ zobrazení přenášející konzistentně[1] strukturu $\mathcal{S}_1$ do $\mathcal{S}_2$, pak říkáme, že zobrazení f **zachovává strukturu na** $(N_1, \mathcal{S}_1)$ a f nazýváme **homomorfizmem** $(N_1, \mathcal{S}_1)$ do $(N_2, \mathcal{S}_2)$; píšeme $f : (N_1, \mathcal{S}_1) \to (N_2, \mathcal{S}_2)$. Homomorfizmus $(N, \mathcal{S})$ do $(N, \mathcal{S})$ se nazývá **endomorfizmus struktury** $(N, \mathcal{S})$. Bijektivní homomorfizmus se nazývá **izomorfizmus**, jestliže $f^{-1} : (N_2, \mathcal{S}_2) \to (N_1, \mathcal{S}_1)$ je rovněž homomorfizmem. V takovém případě píšeme $(N_1, \mathcal{S}_1) \simeq (N_2, \mathcal{S}_2)$.

2.1. **RELACE A OPERACE.**

DEFINICE 2.3. Buďte $M_1, M_2, \dots, M_n$, $n \in \mathbb{N}$, neprázdné množiny, pak každou podmnožinu $\rho \subseteq M_1 \times M_2 \times \cdots \times M_n$ nazýváme n**-ární relací mezi množinami** $M_1, M_2, \dots, M_n$ (pro $n = 1$ **unární**, pro $n = 2$ **binární**, pro $n = 3$ **ternární** atd.).
Je-li $M_1 = M_2 = \dots M_n =: M$, pak $\rho \subseteq M^n$ nazýváme n**-ární relací na množině** M. Řekneme pak, že (M, ρ) **je množina s relací**. V případě binární relace se obvykle místo $[x, y] \in \rho$ píše $x \, \rho \, y$ a říká se, že **prvek** x **je v relaci** ρ **s prvkem** y. Podobně píšeme $x \, \overline{\rho} \, y$ nebo $x \, \mathrm{non}\rho \, y$, jestliže tomu tak není.

DEFINICE 2.4. Buďte M a $M_1, M_2, \dots, M_n$, $n \in \{0\} \cup \mathbb{N}$, neprázdné množiny, pak zobrazení $f : M_1 \times M_2 \times \cdots \times M_n \to M$ nazýváme **funkcí** n **proměnných na** $M_1 \times M_2 \times \cdots \times M_n$.
Je-li $M_1 = M_2 = \dots M_n =: M$, pak $f : M^n \to M$ nazýváme n**-ární operací na množině** M (pro $n = 0$ **nulární**, pro $n = 1$ **unární**, pro $n = 2$ **binární**, pro $n = 3$ **ternární** atd.). Řekneme pak, že (M, f) **je množina s operací**. Píšeme obvykle místo $f([x_1, \dots, x_n])$ zjednodušeně $f(x_1, \dots, x_n)$. V případě binární operace se obvykle místo $y = f(x_1, x_2)$ píše $y = x \, f \, y$, pokud f reprezentuje vhodný operátor (např. + pro operaci sečítání).

[1] Přesný význam určuje každá konkrétní struktura — viz dále

Poznámka 2.5. Někdy také relaci ztotožňujeme s její charakteristickou funkcí (viz 1.5) a v souladu s 2.4 píšeme
$\rho(x_1, x_2, \ldots, x_n) = 1$, resp. $\rho(x_1, x_2, \ldots, x_n) = 0$,
jestliže prvky $x_i \in M_i$ $(i = 1, 2, \ldots, n)$ jsou, resp. nejsou v relaci ρ. Každá unární relace na M koresponduje s nějakou podmnožinou v M. Relační struktury představují základní aparát konstrukce tzv. **relačních databázových systémů**, kde jsou dle potřeby do vzájemného vztahu dávány informace uložené v databázi.

Poznámka 2.6.

(1) Pro danou funkci n proměnných můžeme zavést $(n+1)$-ární relaci $\rho_f \subseteq M_1 \times \cdots \times M_n \times M$ takto: $\rho_f(x_1, \ldots, x_n, y) = 1$ právě když $y = f(x_1, \ldots, x_n)$. Zřejmě ρ_f pak můžeme považovat za **graf funkce** f. Obvykle však neděláme rozdíl mezi funkcí a jejím grafem.
Z definice zobrazení naopak plyne, že daná $(n+1)$-ární relace $\rho \subseteq M_1 \times \cdots \times M_n \times M$ může být grafem nejaké funkce n proměnných $M_1 \times M_2 \times \cdots \times M_n$ do M právě když má tuto vlastnost:
pro každou uspořádanou n-tici $x_1 \in M_1, \ldots, x_n \in M_n$ existuje jediné $y \in M : \rho(x_1, \ldots, x_n, y) = 1$. Funkční hodnotou je pak právě tento prvek y.

(2) Zvláštní roli hraje nulární operace na M. Podle 1.36(4) ji totiž můžeme považovat za zobrazení $M^{\emptyset} \to M$, tj. za zobrazení, které prázdnému zobrazení přiřazuje nějaký **význačný prvek** z M. Opět nerozlišujeme mezi význačným prvkem a nulární operací, která jej vybrala: strukturu s jedním význačným prvkem pak zapisujeme například takto: $(\mathbb{R}, 1)$.

Pokud nebude řečeno jinak, budeme nadále ve zbytku této kapitoly uvažovat algebraické struktury $(M, \mathcal{S})$, kde $\mathcal{S}$ obsahuje pouze relace a operace.

DEFINICE 2.7. Binární relace na M se nazývá:

a) **reflexivní**, když $a\,\rho\,a$ pro každé $a \in M$;
b) **areflexivní**, když $a\,\overline{\rho}\,a$ pro každé $a \in M$;
c) **symetrická**, když $a\,\rho\,b \Rightarrow b\,\rho\,a$ pro libovolné $a, b \in M$;
d) **asymetrická**, když $a\,\rho\,b \Rightarrow b\,\overline{\rho}\,a$ pro libovolné $a, b \in M$;
e) **antisymetrická**, když
$a\,\rho\,b, b\,\rho\,a \Rightarrow a = b$ pro libovolné $a, b \in M$;
f) **tranzitivní**, když $a\,\rho\,b, b\,\rho\,c \Rightarrow a\,\rho\,c$ pro libovolné $a, b, c \in M$;
g) **atranzitivní** $a\,\rho\,b, b\,\rho\,c \Rightarrow a\,\overline{\rho}\,c$ pro libovolné $a, b, c \in M$;
h) **antitranzitivní**, když
$a\,\rho\,b, b\,\rho\,c, a\,\rho\,c \Rightarrow (a = b) \vee (b = c) \vee (a = c)$
pro libovolné $a, b, c \in M$;
i) **úplná**, když pro každé $a, b \in M$ platí $a\,\rho\,b$ nebo $b\,\rho\,a$.

DEFINICE 2.8. Binární operace $\circ$ na M se nazývá:

a) **asociativní**, když
$a \circ (b \circ c) = (a \circ b) \circ c$ pro libovolné $a, b, c \in M$;
b) **komutativní**, když $a \circ b = b \circ a$ pro libovolné $a, b \in M$;

Význačný prvek $e \in M$ se nazývá **neutrálním prvkem binární operace** $\circ$, jestliže $a \circ e = e \circ a = a$ pro každé $a \in M$;

Definice 2.9.
Řekneme, že dvě algebraické struktury $(M_1, \mathcal{S}_1)$ a $(M_2, \mathcal{S}_2)$ jsou **téhož typu**, jestliže existuje bijekce $\mathcal{S}_1$ na $\mathcal{S}_2$ přiřazující každé relaci (operaci) z $\mathcal{S}_1$ odpovídající relaci (operaci) v $\mathcal{S}_2$ téže arity.

Definice 2.10. Pro dvě algebraické struktury $(M_1, \mathcal{S}_1)$ a $(M_2, \mathcal{S}_2)$ téhož typu považujeme ve smyslu definice 2.2 za **homomorfizmus** $(M_1, \mathcal{S}_1)$ **do** $(M_2, \mathcal{S}_2)$ každé zobrazení $f : M_1 \to M_2$ s těmito vlastnostmi:

(1) pro každou relaci $\rho_1 \in \mathcal{S}_1$ a odpovídající relaci $\rho_2 \in \mathcal{S}_2$ téže arity n platí: $\rho_1(x_1, \ldots, x_n) = 1 \Rightarrow \rho_2(f(x_1), \ldots, f(x_n)) = 1$;
(2) pro každou operaci $\omega_1 \in \mathcal{S}_1$ a odpovídající operaci $\omega_2 \in \mathcal{S}_2$ téže arity n platí: $f(\omega_1(x_1, \ldots, x_n)) = \omega_2(f(x_1), \ldots, f(x_n))$.

Zejména f zobrazí každý význačný prvek v $(M_1, \mathcal{S}_1)$ na odpovídající význačný prvek v $(M_2, \mathcal{S}_2)$. Zřejmě složení dvou homomorfizmů je opět homomorfizmus (viz též dále konec poznámky 2.61).

Definice 2.11 (Přímý součin algebraických struktur)**.**
Nechť $\{(M_i, \mathcal{S}_i)\}_{i \in I}$ je systém algebraických struktur téhož typu: $\mathcal{S}_i = \{\rho_{ij}\}_{j \in J}$, kde ρ_{ij} je pro každé $i \in I$ buď operace nebo relace téže arity n_j. Algebraickou strukturu $(M, \mathcal{S})$ nazveme **přímým součinem** algebraických struktur $(M_i, \mathcal{S}_i)$, jestliže $M = \mathop{\mathrm{X}}_{i \in I} M_i$, kde $\mathcal{S} := \{\rho_j\}_{j \in J}$ obsahuje relace (operace) definované po složkách: nechť $\varphi, \varphi_k \in M$ pro $k = 1, \ldots, n_j$ a $j \in J$, pak

(1) jsou-li ρ_{ij} relace pro každé $i \in I$, definujeme j-tou relaci takto:
$\rho_j(\varphi_1, \ldots, \varphi_{n_j}) = 1$ právě když $\rho_{ij}(\varphi_1(i), \ldots, \varphi_{n_j}(i)) = 1$ pro všechna $i \in I$;
(2) jsou-li ρ_{ij} operace pro každé $i \in I$, definujeme j-tou operaci takto:
$\rho_j(\varphi_1, \ldots, \varphi_{n_j})(i) := \rho_{ij}(\varphi_1(i), \ldots, \varphi_{n_j}(i))$ pro každé $i \in I$.

Značíme také $\mathcal{S} =: \mathop{\mathrm{X}}_{i \in I} \mathcal{S}_i$, případně $(M, \mathcal{S}) =: \mathop{\mathrm{X}}_{i \in I} (M_i, \mathcal{S}_i)$.
Je-li I konečná, například $I = \{1, 2, \ldots, q\}$, pak také explicitně:
$\mathcal{S} =: \mathcal{S}_1 \times \mathcal{S}_2 \times \cdots \times \mathcal{S}_q$ a $(M, \mathcal{S}) =: (M_1, \mathcal{S}_1) \times (M_2, \mathcal{S}_2) \times \cdots \times (M_q, \mathcal{S}_q)$.

Definice 2.12 (Algebraické podstruktury)**.**
Nechť $(M, \mathcal{S})$ a $(M', \mathcal{S}')$ jsou algebraické struktury téhož typu: $\mathcal{S} = \{\rho_j\}_{j \in J}$ a $\mathcal{S}' = \{\rho'_j\}_{j \in J}$, kde ρ_j a ρ'_j jsou pro každé $j \in J$ buď operacemi nebo relacemi téže arity n_j. Řekneme, že $(M', \mathcal{S}')$ je **algebraickou podstrukturou** algebraické struktury $(M, \mathcal{S})$, jestliže $M' \subseteq M$ a pro každé $j \in J$ a $x_1, \ldots, x_{n_j} \in M'$ platí:

(1) jsou-li ρ_j a ρ'_j relace, pak
$\rho'_j(x_1, \ldots, x_{n_j}) = 1$ právě když $\rho_j(x_1, \ldots, x_{n_j}) = 1$, neboli $\rho'_j = M'^{n_j} \cap \rho_j$;
(2) jsou-li ρ_j a ρ'_j operace, pak
$x := \rho_j(x_1, \ldots, x_{n_j}) \in M'$ a $\rho'_j(x_1, \ldots, x_{n_j}) = x$.

Říkáme také, že podmnožina $M' \subseteq M$ je **uzavřená vzhledem ke struktuře** $\mathcal{S}$ a píšeme $(M', \mathcal{S}') \subseteq (M, \mathcal{S})$ nebo jen $M' \subseteq M$. Zejména M' musí obsahovat všechny význačné prvky z M.

Definice 2.13 (Generátory)**.**
Nechť $(M, \mathcal{S})$ je algebraická struktura a $G \subseteq M$ nějaká její podmnožina. Jestliže existuje nejmenší[2] podmnožina $M^* \subseteq M$ obsahující G (tj. $G \subseteq M^*$) taková, že $(M^*, \mathcal{S})$ je podstrukturou v $(M, \mathcal{S})$, pak G nazýváme **množinou generátorů struktury** $(M^*, \mathcal{S})$ nebo také říkáme, že **struktura** $(M^*, \mathcal{S})$ **je generována svou podmnožinou** G a píšeme $M^* = \mathcal{S}(G)$ (zde $\mathcal{S}$ vystupuje spíše v roli symbolu pro struktury téhož typu).

Příklad 2.14. $(\mathbb{N}, +)$ je algebraická podstruktura v $(\mathbb{Z}, +)$ generovaná jednoprvkovou podmnožinou $G = \{1\} \subseteq \mathbb{Z}$.

Poznámka 2.15. Binární relace či operace na konečných množinách nevelkého rozsahu lze zadat tabulkou (viz `[KaSk:obr.8,15 s.26,45]`). Binární relace je také možno znázornit graficky (`[KaSk:obr.9 s.27]`). V dalších odstavcích této kapitoly se již zaměříme na speciální případy jednoduchých struktur, které spolu s příklady budou dobře ilustrovat obecnou koncepci, kterou jsme zavedli v tomto odstavci.

2.2. USPOŘÁDANÉ MNOŽINY.

DEFINICE 2.16. Binární relace ρ na M se nazývá **(částečné) uspořádání**, je-li reflexivní, antisymetrická a tranzitivní. Nazývá se **úplné uspořádání** nebo také **lineární uspořádání**, je-li navíc úplná. Algebraická struktura (M, ρ) se pak nazývá **(částečně, příp. lineárně) uspořádaná množina**. Relace uspořádání se obvykle značí symbolem $\leq$ nebo $\preceq$ a pod. Píšeme pak $(M, \leq)$ nebo $(M, \preceq)$ a pod.

---

[2] $(M', \mathcal{S}) \subseteq (M, \mathcal{S}), G \subseteq M' \Rightarrow (M^*, \mathcal{S}) \subseteq (M', \mathcal{S})$ ... viz dále 2.20

<u>PŘÍKLAD</u> 2.17.

<u>Lineárně uspořádané množiny:</u>
$(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$ a $(\mathbb{R}, \leq)$ s obvyklým uspořádáním.
<u>Částečně uspořádané množiny, které nejsou lineárně uspořádány:</u>
$(\mathbb{N}, |)$, kde $n|m$ značí, že n je dělitelem m; $(\mathcal{P}(M), \subseteq)$;

<u>Poznámka</u> 2.18. Uspořádané množiny lze graficky znázornit pomocí tzv. **Hasseova diagramu** (viz `[KaSk:obr.11,12 s.28-29]`).

<u>VĚTA</u> 2.19 (Důkaz D.1)**.**
Nechť $\leq$ je uspořádání na M. Definujme na M relaci $<$ takto:
$a < b \;\Leftrightarrow\; (a \leq b) \wedge (a \neq b)$. *Pak $<$ je relace areflexivní a tranzitivní.*
Naopak, je-li $<$ areflexivní a tranzitivní relace na M a definujeme-li $a \leq b \;\Leftrightarrow\; (a < b) \vee (a = b)$, *pak $\leq$ je uspořádání na M.*

<u>DEFINICE</u> 2.20.

Buď $(M, \leq)$ uspořádaná množina. Prvek $a \in M$ se nazývá **nejmenší**, resp. **největší prvek v** M, platí-li $x \geq a$, resp. $x \leq a$ pro každé $x \in M$.
Prvek $a \in M$ se nazývá **minimální**, resp. **maximální** prvek v M, jestliže pro žádné $x \in M$ neplatí $x < a$, resp. $x > a$.

<u>VĚTA</u> 2.21 (Důkaz D.2)**.** `[KaSk:V3.1 s.28]`

(1) *Libovolná uspořádaná množina má nejvýše jeden nejmenší a nejvýše jeden největší prvek.*
(2) *Má-li uspořádaná množina nejmenší, resp. největší prvek, pak tento prvek je zároveň jejím jediným minimálním, resp. maximálním prvkem.*
(3) *V úplně uspořádané množině existuje nejvýše jeden minimální, resp. maximální prvek, který je zároveň jejím nejmenším, resp. největším prvkem.*
(4) *Každá neprázdná konečná uspořádaná množina má alespoň jeden minimální a alespoň jeden maximální prvek.*

Definice 2.22.
Nechť $(M, \leq)$ je uspořádaná množina. Pro prvky $a, b \in M$ řekneme, že b **pokrývá** a, jestliže $a < b$ a neexistuje $c \in M$ tak, že $a < c < b$.

Věta 2.23 (Důkaz D.3)**.**
Nechť $(M, \leq)$ je konečná uspořádaná množina. Pak platí $a < b \Leftrightarrow$ existuje konečný počet prvků $a = t_0 < t_1 < \cdots < t_n = b$ tak, že t_i pokrývá t_{i-1} pro každé $i = 1, \ldots, n$.

DEFINICE 2.24. Buď $(M, \leq)$ uspořádaná množina a $N \subseteq M$. Prvek $a \in M$ se nazývá **dolní**, resp. **horní závora (hranice) podmnožiny** N **(v** M**)**, platí-li $x \geq a$, resp. $x \leq a$ pro každé $x \in N$.

DEFINICE 2.25. Buď $(M, \leq)$ uspořádaná množina a $N \subseteq M$. Prvek $a \in M$ se nazývá **největší dolní závora**, resp. **nejmenší horní závora** neboli **infimum**, resp. **supremum** množiny N (v M), platí-li:

(1) a je dolní, resp. horní závora N,
(2) pro každou dolní, resp. horní závoru t množiny N platí $t \leq a$, resp. $t \geq a$.

Pak píšeme $a = \inf N$, resp. $a = \sup M$. Má-li N nejmenší, resp. největší prvek, pak tento prvek je zřejmě jejím infimem, resp. supremem.

DEFINICE 2.26 (srov. s 1.27 a s 1.28)**.**
Buď $(M, \leq)$ uspořádaná množina a $N := \{a_n\}_{n=1}^{\infty}$ posloupnost jejích prvků. Pokud existuje $b_k^- := \inf\{a_n\}_{n=k}^{\infty}$ pro každé $k \in \mathbb{N}$ i $a^- := \sup_{k \in \mathbb{N}} b_k^-$, pak a^- nazýváme **limes inferior** posloupnosti $\{a_n\}$ a píšeme $a^- = \liminf a_n$.
Analogicky duálně: pokud existuje $b_k^+ := \sup\{a_n\}_{n=k}^{\infty}$ pro každé $k \in \mathbb{N}$ i $a^+ := \inf_{k \in \mathbb{N}} b_k^+$, pak a^+ nazýváme **limes superior** posloupnosti $\{a_n\}$ a píšeme $a^+ = \limsup a_n$. Pokud existuje a^- i a^+, pak platí $\liminf a_n \leq \limsup a_n$ (CVIČENÍ: návod D.4). Platí-li rovnost, pak jejich společnou hodnotu $a := a^- = a^+$ nazýváme **limitou posloupnosti** $\{a_n\}_{n \in \mathbb{N}}$ a píšeme $a = \lim a_n$. Říkáme také, že **posloupnost** $\{a_n\}_{n=1}^{\infty}$ **konverguje k** a.

VĚTA 2.27 (Důkaz D.5)**.**

(1) *Je-li posloupnost neklesající,* $a_1 \le a_2 \le a_3 \le \dots$, *a existuje* $a := \sup a_n$, *pak* $\lim a_n = a$ *a píšeme také* $a_n \uparrow a$.

(2) *je-li posloupnost nerostoucí,* $a_1 \ge a_2 \ge a_3 \ge \dots$, *a existuje* $a := \inf a_n$, *pak* $\lim a_n = a$ *a píšeme také* $a_n \downarrow a$.

DEFINICE 2.28 (viz 2.2 a 2.10(1))**.**
Buďte $(M, \le)$ a $(N, \preceq)$ uspořádané množiny. Zobrazení $f : M \to N$ se nazývá **homomorfizmus** nebo také **monotonní zobrazení**, jestliže pro libovolné prvky $x, y \in M$, $x \le y$, platí $f(x) \preceq f(y)$. V souladu s 2.2 píšeme $f : (M, \le) \to (N, \preceq)$. Zobrazení f se nazývá **izomorfismus**, jestliže navíc rovněž $f^{-1} : N \to M$ je homomorfizmem, neboli pro libovolné prvky $x, y \in M$ platí $x \le y \;\Leftrightarrow\; f(x) \preceq f(y)$.

Věta 2.29 (Důkaz D.6)**.**
Buďte $(M, \le)$ *a* $(N, \preceq)$ *uspořádané množiny a* $f : (M, \le) \to (N, \preceq)$ *izomorfizmus. Nechť* $P \subseteq M$ *je nějaká podmnožina. Pak* $\inf P$*, resp.* $\sup P$ *existuje v* M *právě když existuje* $\inf f(P)$*, resp.* $\sup f(P)$ *v* N*. V takovém případě platí* $f(\inf P) = \inf f(P)$*, resp.* $f(\sup P) = \sup f(P)$.

Důsledek 2.30. *Nechť v předchozí větě* $P = \{a_n\}_{n=1}^{\infty}$ *je posloupnost. Pak* $\liminf a_n$*, resp.* $\limsup a_n$ *existuje v* M *právě když existuje* $\liminf f(a_n)$*, resp.* $\limsup f(a_n)$ *v* N*. V takovém případě platí* $f(\liminf a_n) = \liminf f(a_n)$*, resp.* $f(\limsup a_n) = \limsup f(a_n)$.

DEFINICE 2.31 (Přímý součin uspořádaných množin – viz 2.11(1))**.**
Nechť $(M, \le)$ a $(N, \le)$ jsou dvě uspořádané množiny a $(M \times N, \le)$ jejich přímý součin. Buďte $[m_1, n_1], [m_2, n_2] \in M \times N$ dva prvky, pak $[m_1, n_1] \le [m_2, n_2] \;\Leftrightarrow\; (m_1 \le m_2) \wedge (n_1 \le n_2)$. Analogicky (po složkách) uspořádáme prvky přímého součinu konečně mnoha uspořádaných množin či libovolného systému takových množin.

2.3. **EKVIVALENCE A KONGRUENCE.**

DEFINICE 2.32.
Binární relace ρ na množině M se nazývá **ekvivalencí** na této množině, jestliže je reflexivní, symetrická a tranzitivní. Obvykle se značí symboly $\sim$, $\equiv$ nebo $\simeq$ a pod. Píšeme pak $(M,\sim)$,$(M,\equiv)$ nebo $(M,\simeq)$ a pod. Množinu všech ekvivalencí na M budeme dále značit $E(M)$. Tato množina je uspořádána inkluzí $\subseteq$ neboli pro ekvivalence $\rho,\sigma \in E(M)$ je $\rho \subseteq \sigma \;\Leftrightarrow\; [x\rho y \Rightarrow x\sigma y]$.

DEFINICE 2.33.
Buď M neprázdná množina. **Rozkladem $\overline{M}$ na množině** M rozumíme neprázdný systém po dvou disjunktních neprázdných podmnožin $\overline{M} := \{M_i\}_{i\in I}$ množiny M, jejichž sjednocením je celá množina M. Prvky $\overline{M}$ se nazývají **třídy tohoto rozkladu**. Vybereme-li z každé třídy M_i nějaký prvek m_i, pak m_i se nazývá **reprezentantem třídy** M_i a množina všech reprezentantů $\{m_i \mid i \in I\}$ se nazývá **systém reprezentantů rozkladu** $\overline{M}$. Přiřadíme-li každému prvku $m \in M$ (jednoznačně určenou) třídu rozkladu $\overline{m}$, do níž m patří, pak toto zobrazení (pruh nahoře) je surjekcí M na $\overline{M}$ a nazývá se **kanonickým zobrazením rozkladu** $\overline{M}$. Jeho restrikce na systém reprezenantů je pak bijekce na $\overline{M}$.

VĚTA 2.34 (Důkaz D.7). `[KaSk:V3.2 s.31]`
Buď $\overline{M}$ rozklad na množině M. Definujme relaci ρ na M takto: $x\rho y \Leftrightarrow$ existuje třída $\overline{m} \in \overline{M}$ tak, že $x \in \overline{m}, y \in \overline{m}$.
Pak ρ je ekvivalence na M.

VĚTA 2.35 (Důkaz D.8). `[KaSk:V3.3 s.31]`
Buď ρ ekvivalence na množině M. Pak existuje jediný rozklad $\overline{M}$ na M takový, že pro $x, y \in M$ platí $x\rho y \;\Leftrightarrow\;$ existuje třída $\overline{m} \in \overline{M}$ tak, že $x \in \overline{m}, y \in \overline{m}$.

DEFINICE 2.36. Rozklad $\overline{M}$ příslušný k ekvivalenci ρ na M popsaný v předchozí větě značíme $\overline{M} =: M/\rho$. Označme $R(M)$ množinu všech rozkladů na množině M.

Definice 2.37. Buďte $\overline{M}, \widetilde{M} \in R(M)$. Pravíme, že $\overline{M}$ **je jemnější než** $\widetilde{M}$, neboli $\widetilde{M}$ **je hrubší než** $\overline{M}$, když ke každé třídě $\overline{m} \in \overline{M}$ existuje třída $\widetilde{m} \in \widetilde{M}$ tak, že $\overline{m} \subseteq \widetilde{m}$. Píšeme $\overline{M} \leq \widetilde{M}$. Snadno nahlédneme, že $\leq$ je uspořádání na $R(M)$.

Věta 2.38 (Důkaz D.9)**.**
Buď M neprázdná množina a pro libovolné $\Theta \in E(M)$ položme $f(\Theta) := M/\Theta$. Pak f je izomorfismus $(E(M), \subseteq)$ na $(R(M), \leq)$.

<u>VĚTA</u> 2.39 (Důkaz D.10)**.**
Nechť M, N jsou neprázdné množiny a $f : M \to N$ zobrazení. Definujme na M relaci $\overset{f}{\sim}$ takto: $x \overset{f}{\sim} y \Leftrightarrow f(x) = f(y)$. Pak $\overset{f}{\sim}$ je ekvivalence na M a třídy rozkladu $M/\overset{f}{\sim}$ jsou právě úplné vzory všech prvků z $f(M)$, tj. $M/\overset{f}{\sim} = \{f^{-1}(\{n\}) \mid n \in f(M)\}$. Zejména dostáváme bijekci (jednojednoznačnou korespondenci) mezi třídami rozkladu, jejich reprezentanty a obrazem $f(M)$ množiny M v N.

<u>DEFINICE</u> 2.40. Rozklad $M/\overset{f}{\sim}$ z předchozí věty se nazývá **kanonický rozklad** příslušný k zobrazení f.

Důsledek 2.41 (Důkaz D.11)**.**
Nechť M, N, P jsou neprázdné množiny a $f : M \to N$ a $g : N \to P$ dvě zobrazení. Označíme-li $gf : M \to P$ složené zobrazení, pak $\overset{f}{\sim} \subseteq \overset{gf}{\sim}$ a tedy kanonický rozklad příslušný k f je vždy jemnější než kanonický rozklad příslušný ke složenému zobrazení gf.

DEFINICE 2.42. Buď dána algebraická struktura $(M, \mathcal{S})$ a nějaká ekvivalence $\sim$ na M. Řekneme, že $\sim$ je **kongruencí** na struktuře $(M, \mathcal{S})$, jestliže pro každou n-ární operaci ω na M, $\omega \in \mathcal{S}$, platí:

(1) $a_1 \sim b_1, \ldots, a_n \sim b_n \Rightarrow \omega(a_1, \ldots, a_n) \sim \omega(b_1, \ldots, b_n)$.

Na $\overline{M} := M/\sim$ lze pak zavést strukturu $\overline{\mathcal{S}}$ stejného typu jako $\mathcal{S}$ takto:

(i) pro každou relaci $\rho \in \mathcal{S}$ n-ární definujeme $\overline{\rho} \in \overline{\mathcal{S}}$ téže arity: $\overline{\rho}(\overline{a}_1, \ldots, \overline{a}_n) := 1$ právě když pro nějaký výběr reprezentantů $a_1, \ldots, a_n$ je $\rho(a_1, \ldots, a_n) = 1$;

(ii) pro každou operaci $\omega \in \mathcal{S}$ n-ární definujeme $\overline{\omega} \in \overline{\mathcal{S}}$ téže arity takto:

a) $n = 0$: význačným prvkem $\overline{\omega}$ je třída obsahující význačný prvek ω,

b) $n > 0$: $\overline{\omega}(\overline{a}_1, \ldots, \overline{a}_n) := \overline{\omega(a_1, \ldots, a_n)}$ pro nějaký výběr reprezentantů $a_1, \ldots, a_n$ (dle (1) na výběru nezáleží).

Strukturu $(\overline{M}, \overline{\mathcal{S}})$ pak značíme $(M, \mathcal{S})/\sim$ a nazýváme ji **faktorovou (podílovou) strukturou struktury** $(M, \mathcal{S})$ **vzhledem ke kongruenci** $\sim$.

VĚTA 2.43 (Důkaz D.12)**.** *Buď dána algebraická struktura $(M, \mathcal{S})$ a nějaká kongruence $\sim$ na M. Pak příslušné kanonické zobrazení je homomorfizmus $(M, \mathcal{S})$ na $(\overline{M}, \overline{\mathcal{S}})$.*

Je-li naopak $f : (M, \mathcal{S}) \to (N, \mathcal{S}')$ nějaký homomorfizmus, pak $\stackrel{f}{\sim}$ v příslušném kanonickém rozkladu $\overline{M} := M/\stackrel{f}{\sim}$ je kongruence na $(M, \mathcal{S})$. Přitom $(f(M), \mathcal{S}')$ je podstruktura v $(N, \mathcal{S}')$ izomorfní s $(\overline{M}, \overline{\mathcal{S}})$.

2.4. STRUKTURY S JEDNOU BINÁRNÍ OPERACÍ.

<u>DEFINICE</u> 2.44. Algebraická struktura $(M, \circ)$ s jednou binární operací $\circ$ se nazývá **grupoid**. Grupoid $(M, \circ)$, v němž platí asociativní zákon se nazývá **pologrupa**. Každá pologrupa, v níž existuje neutrální prvek e se nazývá **monoid** — píšeme $(M, \circ, e)$. Je-li operace $\circ$ multiplikativního typu (například $\cdot, *$), pak hovoříme o **multiplikativním grupoidu (pologrupě, monoidu)**. Je-li aditivního typu (například $+, -$), hovoříme o **aditivním grupoidu (pologrupě, monoidu)**. Neutrální prvek e multiplikativního, resp. aditivního grupoidu se obvykle nazývá jeho **jednotkovým, resp. nulovým prvkem** a místo e se značí 1, resp. 0. Grupoid (pologrupa, monoid) se nazývá **komutativní**, jestliže operace $\circ$ je komutativní.

<u>PŘÍKLAD</u> 2.45.

Nechť S je množina nějakých symbolů, například 26 malých písmen abecedy spolu se znakem _ nahrazujícím mezeru: $S = \{a, b, \dots, z, \_\}$. Označme S^* množinu všech konečných řetězců (posloupností) znaků z S včetně prázdného řetězce, tj. $S^* = \{'s_1 s_2 \dots s_n' \mid s_i \in S \text{ pro } i = 1, \dots, n; n \in \mathbb{N}\} \cup \{''\}$. Nechť $(S^*, \circ, '')$ je algebraická struktura, kde $\circ$ je operace skládání řetězců (konkatenace), tj. například definujeme 'auto_'∘'jede':='auto_jede'. Pak $(S^*, \circ, '')$ je zřejmě nekomutativní monoid, jehož neutrálním prvkem je prázdný řetězec $''$.

VĚTA 2.46 (Obecný asoc. zákon ,`[KaSk:V5.1 s.46]`).
Nechť $(M, \circ)$ je pologrupa a $a_1, a_2, \dots, a_n \in M$. Potom všechny možné součiny vytvořené všemi možnými uzávorkováními posloupnosti $\{a_i\}_{i=1}^n$ jsou rovny jednomu a témuž prvku.

VĚTA 2.47.
Každý grupoid má nejvýše jeden neutrální prvek.

DEFINICE 2.48. Nechť $(M, \circ)$ je grupoid s neutrálním prvkem e. Nechť dále $a \in M$ a nechť pro jisté $b \in M$ platí $a \circ b = b \circ a = e$. Potom b se nazývá **inverzní prvek k** a a značí se a^{-1}. V aditivním grupoidu se obvykle nazývá **prvkem opačným k** a a značí se $-a$.

DEFINICE 2.49. Nechť grupoid $(M, \circ)$ má tyto vlastnosti:

(1) Operace $\circ$ je asociativní (neboli $(M, \circ)$ je pologrupa).
(2) Existuje jednotkový prvek e (neboli $(M, \circ)$ je dokonce monoid).
(3) Ke každému prvku $a \in M$ existuje inverzní prvek a^{-1}.

Potom algebraická struktura $(M, \circ, e)$[3] se nazývá **grupa**: multiplikativní, resp. aditivní dle typu operace. Je-li operace $\circ$ navíc komutativní, pak grupa $(M, \circ, e)$ se nazývá **komutativní grupa** nebo také **abelovská grupa**.

---

[3]Přesněji bychom měli psát $(M, \circ, ^{-1}, e)$, neboť grupa je strukturou s jednou binární operací $\circ$, jednou unární operací $^{-1}$ a jedním neutrálním prvkem e.

<u>VĚTA</u> 2.50. ,[KaSk:V5.11 s.50]
Nechť $(M, \circ, e)$ je grupa. Potom pro každé a je a^{-1} určeno jednoznačně, tj. každý prvek má právě jeden inverzní prvek.

PŘÍKLAD 2.51.

a) Množina komplexních čísel $\mathbb{C}$ s obvyklými operacemi $+$, $\cdot$, $-$ tvoří grupoidy $(\mathbb{C}, +)$, $(\mathbb{C}, \cdot)$, $(\mathbb{C}, -)$. Obvyklé dělení / na množině $\mathbb{C}$ není operace, neboť není definován např. prvek $2/0$. Dělení / je ale operace na množině $\mathbb{C}^*$ všech nenulových komplexních čísel. $(\mathbb{C}^*, /)$ je tedy nekomutativní grupoid. Navíc $(\mathbb{C}, +, 0)$ je abelovská grupa, zatímco $(\mathbb{C}, \cdot, 1)$ je jen komutativním monoidem a $(\mathbb{C}, -, 0)$ pouze nekomutativním grupoidem, neboť odečítání není ani asociativní ani komutativní.
Nenulová čísla $(\mathbb{C}^*, \cdot, 1)$ však již tvoří abelovskou grupu vzhledem k násobení, ne tak $(\mathbb{C}^*, /, 1)$ vzhledem k dělení přestože každý prvek má inverzní (jelikož $a/a = 1$, je dokonce každý prvek inverzní sám k sobě). Dělení totiž není podobně jako odečítání ani asociativní ani komutativní operací.

b) Analogicky jako v a) nechť $+, \cdot, -$ mají obvyklý význam. Pak $(\mathbb{R}, +)$, $(\mathbb{R}, \cdot)$, $(\mathbb{R}, -)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{Q}, -)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}, -)$, jsou grupoidy s obdobnými vlastnostmi jako v a). Je-li / obvyklé dělení na množinách $\mathbb{R}^* = R - \{0\}$, $\mathbb{Q}^* = Q - \{0\}$, jsou $(\mathbb{R}^*, /)$, $(\mathbb{Q}^*, /)$ grupoidy. Naproti tomu / není operace na množině celých nenulových čísel, neboť např. $2/3$ není celé nenulové číslo.
Podobně také $(\mathbb{Z}_N, \oplus, 0)$ je abelovská grupa, $(\mathbb{Z}_N, \odot, 1)$ je komutativní monoid a $(\mathbb{Z}_N, \ominus, 0)$ nekomutativní grupoid s operacemi sečítání $\oplus$, odečítání $\ominus$ a násobení $\odot$ modulo N (viz 1.3).

c) Operace $+$ a $\cdot$ jsou také operace na množině $\mathbb{N}$, tedy $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$ jsou komutativní grupoidy. Naproti tomu $-$ a / nejsou operace na $\mathbb{N}$.

d) Je-li X libovolná množina, pak průnik množin $\cap$, sjednocení množin $\cup$, rozdíl množin $(-)$ a symetrická diference množin $(\div)$ jsou operace na množině všech podmnožin 2^X. Jsou tedy: $(2^X, \cap)$, $(2^X, \cup)$, $(2^X, -)$ a $(2^X, \div)$ grupoidy. Navíc $(2^X, \div, \emptyset)$ je abelovská grupa dle věty 1.26, kde každý prvek je opačný sám k sobě, $(2^X, \cup, \emptyset)$ i $(2^X, \cap, X)$ jsou pouze komutativní monoidy, zatímco $(2^X, -)$ pouze nekomutativní grupoid, neboť rozdíl množin není ani komutativní ani asociativní. Naproti tomu kartézský součin $\times$ není obecně operace na množině 2^X.

e) Nechť X je libovolná neprázdná množina. Symbol X^X označuje systém všech zobrazení množiny X do X. Pro $f \in X^X$, $g \in X^X$ je složené zobrazení $g \circ f$ opět prvkem množiny X^X. Tedy $\circ$ je operace na množině X^X a $(X^X, \circ)$ je (obecně nekomutativní) pologrupa. Označíme-li $I_X : X \to X$ identické zobrazení ($I_X(x) = x$ pro každé $x \in X$), pak $(X^X, \circ, I_X)$ je dokonce monoid. *Prvek $f \in X^X$ má inverzní prvek v monoidu $(X^X, \circ, I)$ právě když f je bijekce. Inverzní prvek k f je pak roven inverznímu zobrazení f^{-1} k zobrazení f.*

VĚTA 2.52 (`[KaSk:V5.8 s.48]`).
Nechť $(M, \circ, e)$ je monoid. Nechť a, $a_1, a_2, \ldots, a_n \in M$ mají inverzní prvky v $(M, \circ)$. Pak platí:

(a) $e^{-1} = e$,
(b) $(a^{-1})^{-1} = a$,
(c) $(a_1 \circ a_2 \circ \ldots \circ a_n)^{-1} = a_n^{-1} \circ a_{n-1}^{-1} \circ \ldots \circ a_1^{-1}$,
(d) *pro $b \in M$ jsou prvky $x = a^{-1} \circ b$, $y = b \circ a^{-1}$ jediná řešení rovnic $a \circ x = b$, $y \circ a = b$ v grupoidu $(M, \circ)$.*

Definice 2.53. Nechť $(M, \circ)$ je grupoid. Jestliže pro každou dvojici prvků $a, b \in M$ existuje jediný prvek x tak, že $a \circ x = b$, pak říkáme, že v grupoidu platí **levý zákon o jednoznačném dělení** (resp. **odečítání** v aditivním případě). Jestliže pro každou dvojici prvků $a, b \in M$ existuje jediný prvek y tak, že $y \circ a = b$, pak říkáme, že v grupoidu platí **pravý zákon o jednoznačném dělení** (resp. **odečítání** v aditivním případě).

Věta 2.54. *Pologrupa $(M, \circ)$ je grupou právě když v ní platí levý i pravý zákon o jednoznačném dělení.*

DEFINICE 2.55. Nechť $(M, \circ)$ je grupoid. Jestliže pro každou trojici prvků $a, x, y \in M$ platí implikace $a \circ x = a \circ y \Rightarrow x = y$, pak říkáme, že v grupoidu platí **levý zákon o krácení** (resp. **rušení** v aditivním případě). Jestliže obdobně $x \circ a = y \circ a \Rightarrow x = y$, pak říkáme, že v grupoidu platí **pravý zákon o krácení** (resp. **rušení** v aditivním případě). Říkáme take, že v $(M, \circ)$ lze **krátit zleva**, případně **zprava**.

VĚTA 2.56 (`[KaSk:V5.13 s.51]`).
V každé grupě lze krátit zleva i zprava.

Označení . Nechť $(G, \circ)$ je pologrupa a nechť $a \in G$. Pro přirozené číslo n položíme:

$$a^n := \underbrace{a \circ a \circ \ldots \circ a}_{n \text{ prvků } a}.$$

Má-li grupoid $(G, \circ)$ jedničku e, položíme:

$$a^0 := e.$$

Nechť $(G, \circ)$ má jedničku a prvek a nechť má inverzní prvek a^{-1} v grupoidu $(G, \circ)$. Pak položíme:

$$a^{-n} := (a^{-1})^n := \underbrace{a^{-1} \circ a^{-1} \circ \ldots \circ a^{-1}}_{n \text{ prvků } a^{-1}}.$$

Pro takto zavedené umocňování platí známá pravidla:
$a^m \circ a^n = a^{m+n}$ a $(a^m)^n = a^{mn}$ (viz `[KaSk:V5.9 s.49]`).
V aditivním grupoidu $a - b := a + (-b)$ a dále píšeme na místo a^n a $-na$ místo a^{-n}, takže výše uvedená pravidla pak přepíšeme takto:
$ma + na = (m + n)a$ a $n(ma) = (nm)a = (mn)a$.

<u>DEFINICE</u> 2.57. Algebraickou podstrukturu grupoidu (pologrupy, monoidu, grupy) nazýváme jeho/jejím **podgrupoidem** (**podpologrupou, podmonoidem, podgrupou**).

<u>*POZNÁMKA*</u> 2.58. Nechť $(M, \circ)$ je grupoid a $N \subseteq M$, $N \neq \emptyset$. Uvažme následující vlastnosti podmnožiny N:

(1) $x, y \in N \Rightarrow x \circ y \in N$ (uzavřenost k binární operaci $\circ$);
(2) je-li e neutrální prvek v $(M, \circ)$, pak $e \in N$
(uzavřenost k nulární operaci vybírající neutrální prvek);
(3) je-li $x \in N$ a x^{-1} k němu inverzní prvek v $(M, \circ)$, pak $x^{-1} \in N$ (uzavřenost k unární operaci $^{-1}$).

Podle definice 2.12 je tedy

a) $(N, \circ)$ podgrupoidem (podpologrupou) grupoidu (pologrupy) $(M, \circ)$ právě když má vlastnost (1);
b) $(N, \circ, e)$ je podmonoidem monoidu $(M, \circ, e)$ právě když má vlastnosti (1) a (2);
c) $(N, \circ, e)$ je podgrupou grupy $(M, \circ, e)$ právě když má vlastnosti (1) a (3) [pak má zřejmě i vlastnost (2)].

Každý monoid (každá grupa) $(M, \circ, e)$ má alespoň dva podmonoidy (dvě podgrupy): $(M, \circ, e)$ a **triviální** podmonoid (podgrupu) $(\{e\}, \circ, e)$.

Věta 2.59.
Nechť $(M, \circ, e)$ je grupa a $N \subseteq M$, $N \neq \emptyset$. Pak následující výroky jsou ekvivalentní:

(1) $(N, \circ, e)$ *je podgrupa v* $(M, \circ, e)$,
(2) $x, y \in N \Rightarrow x \circ y^{-1} \in N$,
(3) $x, y \in N \Rightarrow x^{-1} \circ y \in N$.

PŘÍKLAD 2.60.
<u>Podpologrupy:</u>
• $(\mathbb{N}, +) \subset (\mathbb{Z}, +)$,
• množina všech bijekcí $X \rightarrowtail\!\!\!\!\!\twoheadrightarrow X$ z příkladu 2.51e) je grupou, která je podmonoidem v $(X^X, \circ, I_X)$.
<u>Podgrupy:</u>

- $(\mathbb{Z}, +, 0) \subset (\mathbb{Q}, +, 0) \subset (\mathbb{R}, +, 0) \subset (\mathbb{C}, +, 0)$;
- $(\mathbb{R}^+ - \{0\}, \cdot, 1) \subset (\mathbb{R}^*, \cdot, 1)$ ... viz příklad 2.51b);
- Naopak $(\mathbb{Z}_N, \oplus)$ není ani podgrupoid v $(\mathbb{Z}, +)$.

POZNÁMKA 2.61. Nechť $(M, \circ)$ a $(N, \cdot)$ jsou grupoidy a $f : M \to N$ zobrazení. Uvažme následující vlastnosti zobrazení f:

(1) $x, y \in M \Rightarrow f(x \circ y) = f(x) \cdot f(y)$;
(2) jsou-li e, E neutrální prvky po řadě v $(M, \circ)$ a $(N, \cdot)$, pak $f(e) = E$;
(3) je-li $a \in M$ a a^{-1} k němu inverzní prvek v $(M, \circ)$, pak $f(a^{-1})$ je inverzní k $f(a)$ v $(N, \cdot)$, neboli $f(a^{-1}) = f(a)^{-1}$.

Podle definice 2.10 tedy platí:

a) $f : (M, \circ) \to (N, \cdot)$ je homomorfizmus grupoidů právě když má vlastnost (1);
b) $f : (M, \circ, e) \to (N, \cdot, E)$ je homomorfizmus monoidů právě když má vlastnost (1) a (2);
c) $f : (M, \circ, e) \to (N, \cdot, E)$ je grupový homomorfizmus právě když má vlastnosti (1) a (3) [pak má zřejmě i vlastnost (2)] nebo vlastnosti (1) a (2) [pak má zřejmě i vlastnost (3) uvážíme-li větu 2.50];

Kterýkoli z výše uvedených homomorfizmů je izomorfizmem právě když f je bijekce. Snadno se totiž ověří, že $f^{-1} : N \to M$ je rovněž homomorfizmus z $(N, \cdot)$ do $(M, \circ)$: $f^{-1}(E) = f^{-1}(f(e)) = e$,
$f^{-1}(f(a) \cdot f(b)) = f^{-1}(f(a \circ b)) = a \circ b = f^{-1}(f(a)) \circ f^{-1}(f(b))$.
Tento homomorfizmus je ovšem také izomorfizmem. Poznamenejme, že obdobnou vlastnost mají nejen struktury s jednou binární operací, ale každá struktura obsahující pouze operace a žádnou relaci: každý bijektivní homomorfizmus je pak také automaticky izomorfizmem.

PŘÍKLAD 2.62.

(1) Nechť $(S^*, \circ, '')$ je monoid z příkladu 2.45 a $d : S^* \to \mathbb{Z}$ zobrazení přiřazující každému řetězci jeho délku. Pak d je homomorfizmus nekomutativního monoidu $(S^*, \circ, '')$ do abelovské grupy $(\mathbb{Z}, +, 0)$.

(2) Zobrazení modulo f:=$\langle\cdot\rangle_N$ z odst. 1.3 je grupovým homomorfizmem $(\mathbb{Z},+,0)$ na $(\mathbb{Z}_N,\oplus,0)$. Pak $\stackrel{f}{\sim}$ je grupovou kongruencí příslušného kanonického rozkladu (věta 2.43) a platí:
$a \stackrel{f}{\sim} b$ právě když N je dělitelem $b-a$.

2.5. **STRUKTURY SE DVĚMA BINÁRNÍMI OPERACEMI.**

Tyto struktury již zachycují všechny podstatné vlastnosti běžných číselných oborů.

<u>DEFINICE</u> 2.63. Algebraická struktura $(M, +, \cdot, 0)$ s dvěma binárními operacemi $+$ (aditivní) a $\cdot$ (multiplikativní) se nazývá **okruh**, jestliže jsou splněny následující podmínky:

(1) $(M, +, 0)$ je abelovská grupa;
(2) $(M, \cdot)$ je pologrupa;
(3) Pro libovolnou trojici prvků $a, b, c \in M$ platí distributivní zákony:

$$(a + b) \cdot c = a \cdot c + b \cdot c$$
$$c \cdot (a + b) = c \cdot a + c \cdot b.$$

Okruh $(M, +, \cdot, 0)$ se nazývá **okruhem s jednotkou**, jestliže existuje neutrální prvek $1 \in M$ takový, že $(M, \cdot, 1)$ je monoid. Pak píšeme $(M, +, \cdot, 0, 1)$.
Okruh $(M, +, \cdot, 0)$ se nazývá **komutativní**, jestliže $(M, \cdot)$ je komutatitvní pologrupa.

<u>DEFINICE</u> 2.64.
Algebraickou podstrukturu okruhu nazýváme jeho **podokruhem**.

<u>POZNÁMKA</u> 2.65. Nechť $(M, +, \cdot, 0)$ je okruh a $N \subseteq M$, $N \neq \emptyset$. Podle definice 2.12 a s uvážením poznámky 2.58 tedy vidíme, že $(N, +, \cdot, 0)$ je podokruhem v $(M, +, \cdot, 0)$ právě když platí:

(1) $x, y \in N \Rightarrow x + y \in N$;
(2) $x, y \in N \Rightarrow x \cdot y \in N$;
(3) je-li $x \in N$, pak $-x \in N$.
(4) je-li 1 jednotka okruhu $(M, +, \cdot, 0, 1)$, pak $1 \in N$;

Podle poznámky 2.58 je tedy $(N, +, \cdot, 0)$ podokruhem okruhu $(M, +, \cdot, 0, 1)$ právě když $(N, +, 0)$ je podgrupou v $(M, +, 0)$ a současně $(N, \cdot)$ je podpologrupou v $(M, \cdot)$, případně $(N, \cdot, 1)$ je podmonoidem v $(M, \cdot, 1)$.

VĚTA 2.66. *V každém okruhu $(M, +, \cdot, 0)$ platí pro jeho libovolné prvky $a, b, c \in M$ následující identity:*

$$(a - b) \cdot c = a \cdot c - b \cdot c$$
$$c \cdot (a - b) = c \cdot a - c \cdot b$$
$$a \cdot 0 = 0 \cdot a = 0.$$

Definice 2.67.
Nenulový prvek a okruhu $(M, +, \cdot, 0)$ se nazývá **dělitelem nuly** tohoto okruhu, když v M existuje $b \neq 0$ takové, že $a \cdot b = 0$ nebo $b \cdot a = 0$.

Definice 2.68. Komutativní okruh s jednotkou, který nemá dělitele nuly se nazývá **obor integrity**.

Věta 2.69.
V každém oboru integrity $(M, +, \cdot, 0, 1)$ lze krátit (vzhledem ke komutativitě zleva i zprava) nenulovým prvkem:
$a, b, c \in M, a \neq 0, a \cdot b = a \cdot c \Rightarrow b = c$

Důsledek 2.70. *Je-li $(M, +, \cdot, 0, 1)$ obor integrity, pak $(M - \{0\}, \cdot)$ je komutativní grupoid, v němž platí levý i pravý zákon o krácení.*

Definice 2.71 (Charakteristika oboru integrity)**.**
Nechť $(M, +, \cdot, 0, 1)$ je obor integrity. Jestliže existuje přirozené číslo n tak, že $n1 = 0$, potom řekneme, že obor integrity $(M, +, \cdot, 0, 1)$ **má konečnou charakteristiku**. Nejmenší přirozené číslo s touto vlastností se nazývá **charakteristikou** tohoto oboru integrity.
V opačném případě říkáme, že obor integrity $(M, +, \cdot, 0, 1)$ **má nekonečnou charakteristiku** nebo též **charakteristiku nula**.

Věta 2.72.
Nechť obor integrity $(M, +, \cdot, 0, 1)$ má konečnou charakteristiku n, pak n je prvočíslo.

<u>DEFINICE</u> 2.73.
Okruh s jednotkou $(M, +, \cdot, 0, 1)$, v němž $(M - \{0\}, \cdot, 1)$ je grupa se nazývá **těleso**. Je-li tato grupa komutativní, potom $(M, +, \cdot, 0, 1)$ se nazývá **komutativní těleso** nebo také **pole**.

Věta 2.74.
Pole je oborem integrity.

Věta 2.75.
Každý konečný obor integrity je polem.

Příklad 2.76 (viz 2.51)**.**
• $(\mathbb{N}, +, \cdot, 0, 1) \subset (\mathbb{Z}, +, \cdot, 0, 1) \subset (\mathbb{Q}, +, \cdot, 0, 1) \subset (\mathbb{R}, +, \cdot, 0, 1) \subset$
$\subset (\mathbb{C}, +, \cdot, 0, 1)$ jsou do sebe vnořené obory integrity, z nichž poslední tři jsou dokonce pole nekonečné charakteristiky.
• $(\mathbb{Z}_N, \oplus, \odot, 0, 1)$ je komutativním okruhem s jednotkou, který není podokruhem žádného z výše uvedených okruhů. $(\mathbb{Z}_N, \oplus, \odot, 0, 1)$ je oborem integrity jen když N je prvočíslo. V takovém případě je dokonce polem dle věty 2.75.
• Množina všech polynomů s koeficienty například z $\mathbb{C}$ tvoří rovněž obor integrity vzhledem k obvyklému sečítání a násobení polynomů.
• $(2^X, \div, \cap, \emptyset, X)$ je dle věty 1.26 komutativním okruhem s jednotkou X (totiž $A \cap X = A$ pro každou podmnožinu $A \subseteq X$), který není oborem integrity, pokud X má více jak jeden prvek (pak totiž lze vždy najít dvě různé neprázdné podmnožiny s prázdným průnikem).

<u>POZNÁMKA</u> 2.77.
Nechť $(M, +, \circ, 0)$ a $(N, \oplus, \cdot, 0)$ jsou okruhy (tělesa) a $f : M \to N$ zobrazení. Uvážíme-li 2.61b)c), potom f je homomorfizmem těchto struktur ve smyslu 2.10 právě když jak $f : (M, +, 0) \to (M, \oplus, 0)$ tak i $f : (M, \circ) \to (N, \cdot)$ jsou homomorfizmy, tj. právě když f má následující vlastnosti:

(1) $a, b \in M \Rightarrow f(a + b) = f(a) \oplus f(b)$,
(2) $a, b \in M \Rightarrow f(a \circ b) = f(a) \cdot f(b)$,
(3) $f(0) = 0$ a $f(1) = 1$, pokud oba okruhy mají jednotku.

Poznamenejme ještě, že ve (3) lze podmínku $f(0) = 0$ nahradit podmínkou $a \in M \Rightarrow f(-a) = -f(a)$, a v případě těles i podmínku $f(1) = 1$ podmínkou $0 \neq a \in M \Rightarrow f(a^{-1}) = f(a)^{-1}$.

PŘÍKLAD 2.78. Grupový homomorfizmus f:=$\langle\cdot\rangle_N$ z příkladu 2.62(2) je i okruhovým homomorfizmem $(\mathbb{Z}, +, \cdot, 0, 1)$ na $(\mathbb{Z}_N, \oplus, \odot, 0, 1)$, přičemž $\stackrel{f}{\sim}$ je pak také okruhová kongruence.

ANGLICKÁ TERMINOLOGIE ALGEBRAICKÝCH STRUKTUR

algebraická (pod)struktura ⧫ algebraic (sub)structure
homomorfizmus, endomorfizmus ⧫ homomorphism, endomorphism
izomorfizmus, relace, operace ⧫ isomorphism, relation, operation
nulární, unární, binární, n-ární ⧫ nullary, unary, binary, n-ary
význačný, neutrální ⧫ singular, neutral
reflexivní, symetrická, úplná ⧫ reflexive, symmetric, complete
antisymetrická, tranzitivní ⧫ antisymmetric, transitive
asociativní, komutativní ⧫ associative, commutative
generátor, generovaný podmnožinou ⧫ generator, generated by a set
přímý součin, uspořádaná množina ⧫ direct product, ordered set
částečně (lineárně) uspořádaná ⧫ partially (linearly) ordered
menší (větší) nebo roven než ⧫ less (greater) than or equal to
nejmenší (největší) ⧫ least (greatest)
minimální (maximální) ⧫ minimal (maximal)
dolní (horní) závora ⧫ lower (upper) bound
infimum (supremum) ⧫ infimum (supremum)
limes inferior (limes superior) ⧫ inferior limit (superior limit)
ekvivalence, kongruence ⧫ equivalence, congruence
rozklad na třídy, kanonický ⧫ partition into classes, canonical
faktorová struktura ⧫ factor structure
(pod)grupoid, (pod)pologrupa ⧫ (sub)groupoid, (sub)semigroup
(pod)monoid, pod(grupa) ⧫ (sub)monoid, (sub)group
abelovská grupa ⧫ abelian group
opačný (inverzní) prvek ⧫ negated (inverse) element
nulový (jednotkový) prvek ⧫ zero, null (unit) element
(levý, pravý) zákon o krácení ⧫ (left, right) cancellation law
zákon o jednoznačném dělení ⧫ unique division law
okruh, obor integrity ⧫ ring, domain of integrity
dělitel nuly, charakteristika ⧫ divisor of zero, characteristic
těleso, pole ⧫ division ring, field

Teorie a příklady: `[KaSk: s.54-129]`, `[Šik: s.1-131]`
Příklady: `[Ho:řešené č.16-36; s.17-37]`,
`[Ho:neřešené kap.3-7 s.81-167]`

3.1. VEKTOROVÉ PROSTORY.

DEFINICE 3.1. Nechť $(\mathbb{F}, +, \cdot, 0, 1), 0 \neq 1$ je pole (tzv. **pole skalárů**), jehož prvky budeme nazývat **skaláry**. Nechť $(V, +, 0, S_{\mathbb{F}})$ je algebraická struktura s jednou binární operací $+$, nulovým prvkem 0 a zobrazením $S_{\mathbb{F}} : \mathbb{F} \times V \to V$ určujícím pro každý skalár $\alpha \in \mathbb{F}$ jednu unární operaci $\{\alpha\} \times V \to V$ zapisovanou ve tvaru $S_{\mathbb{F}}(\alpha, \boldsymbol{x}) =: \alpha\boldsymbol{x}$ a nazývanou **násobení skalárem**. Nechť $(V, +, 0)$ je abelovská grupa a pro každé $\alpha, \beta \in \mathbb{F}$ a $\boldsymbol{x}, \boldsymbol{y} \in V$ nechť platí:

(L1) Distributivní zákon vzhledem k sečítání vektorů: $\alpha(\boldsymbol{x} + \boldsymbol{y}) = \alpha\boldsymbol{x} + \alpha\boldsymbol{y}$
(L2) Distributivní zákon vzhledem k sečítání skalárů: $(\alpha + \beta)\boldsymbol{x} = \alpha\boldsymbol{x} + \beta\boldsymbol{x}$
(L3) Asociativní zákon vzhledem k násobení skaláry: $\alpha(\beta\boldsymbol{x}) = (\alpha\beta)\boldsymbol{x}$
(L4) $1\boldsymbol{x} = \boldsymbol{x}$.

Pak algebraická struktura $(V, +, 0, S_{\mathbb{F}})$ se nazývá **vektorový (lineární) prostor nad polem** $\mathbb{F}$, prvky množiny V se nazývají **vektory** a operace $\boldsymbol{x} \mapsto \alpha\boldsymbol{x}$ se nazývá **násobení vektoru $\boldsymbol{x}$** skalárem α. Vektorový prostor se nazývá **reálný (resp. komplexní)**, jestliže $\mathbb{F} = \mathbb{R}$ (resp. $\mathbb{F} = \mathbb{C}$).

Poznámka 3.2.

(1) Jestliže nerozlišujeme mezi skalárem a odpovídající unární operací, pak v souladu s 2.1 můžeme vektorový prostor považovat za algebraickou strukturu $(V, \mathcal{L}_{\mathbb{F}})$, kde $\mathcal{L}_F = \{+, (-), 0\} \cup \mathbb{F}$ představuje popis operací lineární struktury (symbol $(-)$ značí unární operaci výběru opačného prvku v aditivní grupě).

(2) Bude-li pole skalárů zřejmé z kontextu, budeme psát též stručně $\mathcal{L}$ místo $\mathcal{L}_{\mathbb{F}}$. V dalším budeme často pracovat s reálným nebo komplexním vektorovým prostorem, kde $\mathcal{L} := \mathcal{L}_{\mathbb{R}}$ nebo $\mathcal{L} := \mathcal{L}_{\mathbb{C}}$.

(3) Pojem vektorového prostoru lze zavést i nad nekomutativním tělesem $\mathbb{F}$. V takovém případě je nutno rozlišovat mezi násobením skaláry zleva a zprava a zavést tzv. **levý (resp. pravý) vektorový prostor nad** $\mathbb{F}$. Je-li $\mathbb{F}$ pouze okruh s $1 \neq 0$, pak se toto pojetí dále zobecňuje a zavádí se tzv. **levý (resp. pravý) modul nad** $\mathbb{F}$ (nebo též $\mathbb{F}$**-modul**).

<u>VĚTA</u> 3.3 (Důkaz D.13). `[Šik:V3.6 s.25]`
Nechť V je vektorový prostor nad $\mathbb{F}$ a $\alpha, \beta, \alpha_i \in \mathbb{F}$; $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{x}_j \in V$.
Pak platí:

(L5) $\alpha \boldsymbol{x} = \boldsymbol{0} \;\Leftrightarrow\; \alpha = 0$ *nebo* $\boldsymbol{x} = \boldsymbol{0}$
(L6) $-\alpha \boldsymbol{x} = \alpha(-\boldsymbol{x}) = (-\alpha)\boldsymbol{x}$
(L7) $\alpha(\boldsymbol{x} - \boldsymbol{y}) = \alpha \boldsymbol{x} - \alpha \boldsymbol{y}$
(L8) $(\alpha - \beta)\boldsymbol{x} = \alpha \boldsymbol{x} - \beta \boldsymbol{x}$
(L9) $\alpha(\boldsymbol{x}_1 + \cdots + \boldsymbol{x}_n) = \alpha \boldsymbol{x}_1 + \cdots + \alpha \boldsymbol{x}_n$
(L10) $(\alpha_1 + \cdots + \alpha_m)\boldsymbol{x} = \alpha_1 \boldsymbol{x} + \cdots + \alpha_m \boldsymbol{x}$
(L11) $\big(\sum_{i=1}^m \alpha_i\big)\big(\sum_{j=1}^n \boldsymbol{x}_j\big) = \sum_{i=1}^m \alpha_i \sum_{j=1}^n \boldsymbol{x}_j = \sum_{i=1}^m \sum_{j=1}^n \alpha_i \boldsymbol{x}_j = \sum_{j=1}^n (\sum_{i=1}^m \alpha_i) \boldsymbol{x}_j$

<u>PŘÍKLAD</u> 3.4 (`[Šik:Př.3.5 s.25]`).

(1) $(\mathbb{F}, \mathcal{L}_{\mathbb{F}})$ je vektorový prostor nad polem $\mathbb{F}$. Vlastnosti (L1) a (L2) jsou důsledkem okruhových distributivních zákonů, (L3) plyne z asociativity okruhového násobení a (L4) rovněž platí, neboť 1 je jednotkou okruhového násobení. Zejména $(\mathbb{R}, \mathcal{L}_{\mathbb{R}})$, resp. $(\mathbb{C}, \mathcal{L}_{\mathbb{C}})$ je reálný, resp. komplexní vektorový prostor.

(2) Užitím přímého součinu z definice 2.11 lze konstruovat další (vícerozměrné) vektorové prostory ($n \in \mathbb{N}, n > 1$):
$(\mathbb{F}^n, \mathcal{L}_{\mathbb{F}}) := \underbrace{(\mathbb{F}, \mathcal{L}_{\mathbb{F}}) \times \cdots \times (\mathbb{F}, \mathcal{L}_{\mathbb{F}})}_{n\times} \ldots n$-tice skalárů z $\mathbb{F}$.

Zejména $(\mathbb{R}^n, \mathcal{L}_{\mathbb{R}})$ (resp. $(\mathbb{C}^n, \mathcal{L}_{\mathbb{C}})$) je reálný (resp. komplexní) vektorový prostor n-tic reálných (resp. komplexních) čísel. V těchto prostorech jsou tedy dle 2.11 všechny operace definovány po složkách:

$[x_1, \dots, x_n] + [y_1, \dots, y_n] := [x_1 + y_1, \dots, x_n + y_n]$
$\mathbf{0} := [0, \dots, 0]$ ... nulový vektor
$-[x_1, \dots, x_n] := [-x_1, \dots, -x_n]$ ... opačný vektor
$\alpha[x_1, \dots, x_n] := [\alpha x_1, \dots, \alpha x_n]$ ... skalární násobek

(3) Analogicky: $(\mathbb{R}^{\mathbb{N}}, \mathcal{L}_{\mathbb{R}}) := \mathop{\mathrm{X}}\limits_{n \in \mathbb{N}} (\mathbb{R}, \mathcal{L}_{\mathbb{R}})$ a $(\mathbb{C}^n, \mathcal{L}_{\mathbb{C}}) := \mathop{\mathrm{X}}\limits_{n \in \mathbb{N}} (\mathbb{C}, \mathcal{L}_{\mathbb{C}})$ jsou po řadě vektorové prostory všech reálných, resp. komplexních posloupností s operacemi po složkách jako ve (2).

(4) Analogicky: $(\mathbb{R}^{I}, \mathcal{L}_{\mathbb{R}}) := \mathop{\mathrm{X}}\limits_{n \in I} (\mathbb{R}, \mathcal{L}_{\mathbb{R}})$ a $(\mathbb{C}^n, \mathcal{L}_{\mathbb{C}}) := \mathop{\mathrm{X}}\limits_{n \in I} (\mathbb{C}, \mathcal{L}_{\mathbb{C}})$ jsou po řadě vektorové prostory všech reálných, resp. komplexních funkcí definovaných na množině I (tj. funkcí z I do $\mathbb{R}$, resp. z I do $\mathbb{C}$) opět s operacemi po složkách. Tedy definujeme pro každé $i \in I$:
$(f + g)(i) := f(i) + g(i), \quad (-f)(i) := -f(i),$
$f \equiv 0 \;\Leftrightarrow\; f(i) = 0$ pro každé $i \in I$,
$(\alpha f)(i) := \alpha f(i)$.

(5) Označme po řadě $\mathbb{R}[t]$, resp. $\mathbb{C}[z]$ množinu všech polynomů jedné proměnné $t \in \mathbb{R}$, resp. $z \in \mathbb{C}$ s koeficienty z $\mathbb{R}$, resp. z $\mathbb{C}$. Pak tyto množiny tvoří vzhledem k obvyklému sečítání a násobení skalárem reálný, resp. komplexní vektorový prostor, který lze ztotožnit s reálnými, resp. komplexními posloupnostmi koeficientů (viz (3)) tvaru $\{a_0, a_1, \dots, a_n, 0, \dots, 0, \dots\}$ pro libovolné $n \in \mathbb{N}$. Omezíme-li se na pevné n, dostaneme vektorové prostory $\mathbb{R}_n[t]$, resp. $\mathbb{C}_n[z]$ všech polynomů s reálnými, resp. komplexními koeficienty stupně nejvýše n.

<u>DEFINICE</u> 3.5.
Nechť $(V, \mathcal{L}_{\mathbb{F}})$ je vektorový prostor, $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n \in V$ a $\alpha_1, \dots, \alpha_n \in \mathbb{F}$. Pokud $\boldsymbol{x} \in V$ lze vyjádřit ve tvaru $\boldsymbol{x} = \alpha_1 \boldsymbol{x}_1 + \dots + \alpha_n \boldsymbol{x}_n$, pak řekneme, že **vektor $\boldsymbol{x}$ je lineární kombinací vektorů $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$.**

3.2. VEKTOROVÉ PODPROSTORY, GENERÁTORY.

DEFINICE 3.6.
Algebraickou podstrukturu (definice 2.12) vektorového prostoru $(V, \mathcal{L}_{\mathbb{F}})$ nazýváme **jeho vektorovým (lineárním) podprostorem**.

VĚTA 3.7 (Důkaz D.14).
Nechť $(V, \mathcal{L}_{\mathbb{F}})$ je vektorový prostor a $\emptyset \neq W \subseteq V$ jeho podmnožina. Pak $(W, \mathcal{L}_{\mathbb{F}})$ je vektorovým podprostorem prostoru $(V, \mathcal{L}_{\mathbb{F}})$ (píšeme $(W, \mathcal{L}_{\mathbb{F}}) \subseteq (V, \mathcal{L}_{\mathbb{F}})$) právě když má následující vlastnosti:

(1) $\boldsymbol{x}, \boldsymbol{y} \in W \Rightarrow \boldsymbol{x} + \boldsymbol{y} \in W$
(uzavřenost vzhledem ke grupovému sečítání)

(2) $\boldsymbol{x} \in W, \alpha \in \mathbb{F} \Rightarrow \alpha \boldsymbol{x} \in W$
(uzavřenost vzhledem ke skalárnímu násobení).

DŮSLEDEK 3.8 (Důkaz D.15).
Každý vektorový podprostor $(W, \mathcal{L}_{\mathbb{F}})$ prostoru $(V, \mathcal{L}_{\mathbb{F}})$ je uzavřený k libovolným lineárním kombinacím svých prvků, tj. platí:
$\boldsymbol{x}_i \in W, \alpha_i \in \mathbb{F}$ *pro* $i = 1, \ldots, n \Rightarrow \alpha_1 \boldsymbol{x}_1 + \cdots + \alpha_n \boldsymbol{x}_n \in W$.

Poznámka 3.9.
V každém vektorovém prostoru $(V, \mathcal{L}_{\mathbb{F}})$ existuje nejmenší vektorový podprostor $(\{\mathbf{0}\}, \mathcal{L}_{\mathbb{F}})$ nazývaný také **nulový podprostor** a největší podprostor totožný s celým prostorem $(V, \mathcal{L}_{\mathbb{F}})$.

VĚTA 3.10 (Důkaz D.16).
Nechť $\{(W_i, \mathcal{L}_{\mathbb{F}})\}_{i \in I}$ je systém vektorových podprostorů prostoru $(V, \mathcal{L}_{\mathbb{F}})$. Pak jejich průnik $\bigcap_{i \in I} W_i$ je rovněž vektorový podprostor ve V.

DEFINICE 3.11. Nechť $(V, \mathcal{L}_{\mathbb{F}})$ je vektorový prostor a $G \subseteq V$ jeho podmnožina. Pak v souladu s definicí 2.13 nejmenší vektorový podprostor ve V obsahující G nazveme **podprostorem generovaným množinou** G nebo také **lineárním obalem množiny** G **ve** V. Značíme jej $\mathcal{L}_{\mathbb{F}}(G)$ nebo stručněji $\mathcal{L}(G)$. Prvky množiny G nazýváme **generátory tohoto podprostoru**.

__**VĚTA**__ **3.12** (Důkaz D.17).
Nechť $(V, \mathcal{L}_{\mathbb{F}})$ *je vektorový prostor a* $G \subseteq V$ *jeho podmnožina. Pak* $\mathcal{L}(G)$ *vždy existuje a platí:*

(1) $\mathcal{L}(G) = \bigcap\{W \mid (W, \mathcal{L}_{\mathbb{F}}) \subseteq (V, \mathcal{L}_{\mathbb{F}}) : G \subseteq W\}$
(neboli $\mathcal{L}(G)$ *je průnikem podprostorů ve* V *obsahujících* G*)*

(2) *Je-li* $G \neq \emptyset$*, pak*
$\mathcal{L}(G) = \{\sum_{i=1}^{n} \alpha_i \boldsymbol{x}_i \mid \alpha_i \in \mathbb{F}, \boldsymbol{x}_i \in G \text{ pro } i = 1, \ldots, n; n \in \mathbb{N}\}$
(neboli $\mathcal{L}(G)$ *tvoří všechny lineární kombinace vektorů z* G*).*

Zejména $\mathcal{L}(\emptyset) = \{\mathbf{0}\}$ *je nulový podprostor.*

__*Poznámka*__ 3.13. Podle 3.12(2) tedy zápis $\boldsymbol{x} \in \mathcal{L}(G)$ vyjadřuje fakt, že $\boldsymbol{x}$ je nějakou lineární kombinací vektorů z množiny G.

__**VĚTA**__ **3.14** (Vlastnosti generátorů, důkaz D.18).
Nechť $(V, \mathcal{L}_{\mathbb{F}})$ *je vektorový prostor,* W *jeho podprostor a* M, N, G *podmnožiny ve* V*. Pak platí:*

(1) $\mathbf{0} \in \mathcal{L}(G)$ *pro každé* $G \subseteq V$
(2) $M \subseteq \mathcal{L}(G) \Rightarrow \mathcal{L}(M) \subseteq \mathcal{L}(G)$
(3) $M \subseteq N \Rightarrow \mathcal{L}(M) \subseteq \mathcal{L}(N)$
(4) $W = \mathcal{L}(W)$ *a zejména* $\mathcal{L}(M) = \mathcal{L}(\mathcal{L}(M))$
(5) *je-li nějaký generátor lineární kombinací ostatních generátorů, pak jej lze vynechat:*
$\boldsymbol{x} \in G,\ \boldsymbol{x} \in \mathcal{L}(G - \{\boldsymbol{x}\}) \Rightarrow \mathcal{L}(G - \{\boldsymbol{x}\}) = \mathcal{L}(G)$.
(6) *každý generátor lze zaměnit za jeho nenulový skalární násobek:*
$\boldsymbol{x} \in G,\ 0 \neq \alpha \in \mathbb{F} \Rightarrow \mathcal{L}((G - \{\boldsymbol{x}\}) \cup \{\alpha\boldsymbol{x}\}) = \mathcal{L}(G)$.
(7) *ke každému generátoru lze přičíst libovolnou lineární kombinaci ostatních generátorů:*
$\boldsymbol{x} \in G,\ \boldsymbol{y} \in \mathcal{L}(G - \{\boldsymbol{x}\}) \Rightarrow \mathcal{L}((G - \{\boldsymbol{x}\}) \cup \{\boldsymbol{x} + \boldsymbol{y}\}) = \mathcal{L}(G)$.

Úpravy uvedené v (5) až (7) se nazývají **elementární úpravy množiny generátorů**.

3.3. **ZÁVISLOST, NEZÁVISLOST, BÁZE, DIMENZE.**

<u>DEFINICE</u> 3.15. Minimální podmnožina ve V generující vektorový prostor $(V, \mathcal{L}_{\mathbb{F}})$ se nazývá **báze tohoto prostoru**, neboli platí implikace: G báze ve $V, M \subseteq G$ systém generátorů prostoru $V \Rightarrow M = G$. Zejména za bázi nulového prostoru tedy můžeme považovat prázdnou množinu.

<u>DEFINICE</u> 3.16.
Nechť $(V, \mathcal{L}_{\mathbb{F}})$ je vektorový prostor a $M := \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\} \subseteq V$ jeho nějaká neprázdná konečná podmnožina navzájem různých vektorů. Řekneme, že M je (resp. vektory $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ jsou) **lineárně nezávislá(é)**, jestliže nulový vektor nelze vyjádřit jako netriviální lineární kombinaci těchto vektorů, tj.:

$$\alpha_i \in \mathbb{F}, i = 1, \ldots, n; \alpha_1 \boldsymbol{x}_1 + \cdots + \alpha_n \boldsymbol{x}_n = \mathbf{0} \quad \Rightarrow \quad \alpha_1 = \cdots = \alpha_n = 0.$$

Nekonečná podmnožina ve V se nazývá **lineárně nezávislá**, jestliže každá její neprázdná konečná podmnožina je lineárně nezávislá. Podmnožina (resp. vektory) vektorového prostoru V se nazývá (nazývají) **lineárně závislá(é)**, jestliže není (nejsou) lineárně nezávislá(é).

<u>VĚTA</u> 3.17 (Důkaz D.19)**.** *Jestliže M je lineárně nezávislá množina nějakého vektorového prostoru, pak platí:*

1. *Každá neprázdná podmnožina v M je lineárně nezávislá;*
2. $\mathbf{0} \notin M$*;*
3. *Je-li $M =: \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ konečná, $\boldsymbol{x} \in \mathcal{L}(M)$ a* $\boldsymbol{x} = \sum_{i=1}^n \alpha_i \boldsymbol{x}_i = \sum_{i=1}^n \beta_i \boldsymbol{x}_i$*, pak $\alpha_i = \beta_i$ pro $i = 1, \ldots, n$.*
4. *Každý vektor $\mathbf{0} \neq \boldsymbol{x} \in \mathcal{L}(M)$ má až na pořadí sčítanců* **jediné** *vyjádření ve tvaru lineární kombinace s nenulovými koeficienty a navzájem různými vektory z M.*

<u>VĚTA</u> 3.18 (Důkaz D.20)**.**
Neprázdná podmnožina M vektorového prostoru $(V, \mathcal{L}_{\mathbb{F}})$ je lineárně závislá právě když existuje vektor $\boldsymbol{x} \in M$, který je lineární kombinací některých dalších vektorů z M, tj. $\boldsymbol{x} \in \mathcal{L}(M - \{\boldsymbol{x}\})$.

<u>VĚTA</u> 3.19 (Důkaz D.21). `[Šik:V3.18,V3.25 s.27-29]`
Nechť $\emptyset \neq G \subseteq V$ je podmnožina nenulového vektorového prostoru $(V, \mathcal{L}_{\mathbb{F}})$. Pak následující výroky jsou ekvivalentní:

(1) *G je báze ve V.*
(2) *G je maximální lineárně nezávislá podmnožina ve V.*
(3) *G je lineárně nezávislá a generuje V, tj. $\mathcal{L}(G) = V$.*

<u>DŮSLEDEK</u> 3.20 (Důkaz D.22). `[Šik:V3.22 s.28]`
Z každé množiny generátorů G nenulového vektorového prostoru V lze vybrat bázi prostoru V jako maximální nezávislou podmnožinu v G. Dokonce to lze udělat tak, aby obsahovala jakoukoli předem danou nezávislou podmnožinu v G.

VĚTA 3.21 (Steinitzova věta o výměně, `[Šik:V3.23 s.28]`,).
Nechť M, N jsou konečné podmnožiny vektorového prostoru $(V, \mathcal{L}_{\mathbb{F}})$, $M \subseteq \mathcal{L}(N)$ lineárně nezávislá. Potom v N existuje podmnožina N' s těmito vlastnostmi:

(1) *N' má týž počet prvků jako M,*
(2) *$\mathcal{L}((N - N') \cup M) = \mathcal{L}(N)$.*

<u>DŮSLEDEK</u> 3.22 (Důkaz D.23). `[Šik:3.26 s.29]`
Má-li nenulový vektorový prostor $(V, \mathcal{L}_{\mathbb{F}})$ konečný systém generátorů, pak ve V existuje konečná báze a všechny báze mají týž (konečný) počet prvků.

<u>DEFINICE</u> 3.23. Má-li vektorový prostor $(V, \mathcal{L}_{\mathbb{F}})$ konečnou bázi o n prvcích. Pak (jednoznačně určené) číslo n nazýváme **dimenzí tohoto prostoru** a píšeme $\dim V = n$. Prostor V pak nazýváme **n-rozměrným (n-dimenzionálním) vektorovým prostorem** nebo také **konečně rozměrným (konečně dimenzionálním) vektorovým prostorem**. Zejména s uvážením definice 3.15 má každý nulový prostor dimenzi 0 (jeho báze je totiž prázdná množina). Vektorový prostor V, v němž neexistuje konečný systém generátorů se nazývá **nekonečně rozměrný (nekonečně dimenzionální)**, píšeme $\dim V = \infty$.

<u>DŮSLEDEK</u> 3.24 (Další důsledky Steinitzovy věty, Důkaz D.24). `[Šik:V3.31-2 s.30]`

(1) *Pro každou lineárně nezávislou množinu vektorů $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$ vektorového prostoru V platí $k \le \dim V$, přičemž každou takovou množinu lze doplnit (rozšířit) na bázi prostoru V.*

(2) *Každý vektorový prostor má bázi.*

(3) *Pro každý lineární podprostor W vektorového prostoru V platí* $\dim W \le \dim V$. *Přitom každou bázi ve W lze rozšířit na bázi ve V. Je-li* $\dim V < \infty$ *a* $W \ne V$, *pak* $\dim W < \dim V$.

(4) *Nechť V je vektorový prostor,* $\dim V = n$, $0 < n < \infty$, *a G jeho podmnožina. Pak následující výroky jsou ekvivalentní:*
   (i) *G je báze ve V.*
   (ii) *G je n-prvková a lineárně nezávislá.*
   (iii) *G je n-prvková a generuje V.*

<u>PŘÍKLAD</u> 3.25.

Pro vektorové prostory z příkladu 3.4 platí:

(1) pro každé $n \in \mathbb{N}$: $(\mathbb{Q}^n, \mathcal{L}_\mathbb{Q}) \subseteq (\mathbb{R}^n, \mathcal{L}_\mathbb{Q})$, $(\mathbb{R}^n, \mathcal{L}_\mathbb{R}) \subseteq (\mathbb{C}^n, \mathcal{L}_\mathbb{R})$, $(\mathbb{R}_n[t], \mathcal{L}_\mathbb{R}) \subseteq (\mathbb{R}[t], \mathcal{L}_\mathbb{R})$, $(\mathbb{C}_n[z], \mathcal{L}_\mathbb{C}) \subseteq (\mathbb{C}[z], \mathcal{L}_\mathbb{C})$.

(2) pro každé $n \in \mathbb{N}$:
$(\mathbb{Q}^n, \mathcal{L}_\mathbb{R}) \nsubseteq (\mathbb{R}^n, \mathcal{L}_\mathbb{R})$, $(\mathbb{R}^n, \mathcal{L}_\mathbb{C}) \nsubseteq (\mathbb{C}^n, \mathcal{L}_\mathbb{C})$, $(\mathbb{R}^n, \mathcal{L}_\mathbb{R}) \nsubseteq (\mathbb{C}^n, \mathcal{L}_\mathbb{C})$, $(\mathbb{R}[z], \mathcal{L}_\mathbb{C}) \nsubseteq (\mathbb{C}[z], \mathcal{L}_\mathbb{C})$, $(\mathbb{R}[z], \mathcal{L}_\mathbb{R}) \nsubseteq (\mathbb{C}[z], \mathcal{L}_\mathbb{C})$.

(3) $\{1\}$ je báze v $(\mathbb{F}, \mathcal{L}_\mathbb{F})$ a tedy $\dim \mathbb{F} = 1$. Zejména $\dim \mathbb{R} = \dim \mathbb{C} = 1$. Podle věty 3.14(6) je bází také každá jednoprvková podmnožina $\{a\}$, $a \ne 0$.

(4) $\mathcal{E}_n := \{[1, 0, \ldots, 0], [0, 1, \ldots, 0], \ldots, [0, 0, \ldots, 1]\}$ je tzv. **přirozená báze** v $(\mathbb{F}^n, \mathcal{L}_\mathbb{F})$. Pro každé $i = 1, \ldots, n$ bude nadále $\varepsilon_i := [0, \ldots, \underset{\stackrel{\uparrow}{i}}{1}, \ldots, 0]$ značit i-tý prvek této báze. Zejména tedy $\dim \mathbb{R}^n = \dim \mathbb{C}^n = n$. Opět podle věty 3.14(6) a s uvážením 3.24(4) je bází také každá podmnožina $\{a_1\varepsilon_1, \ldots, a_n\varepsilon_n\}$, kde $a_i \ne 0$ pro $i = 1, \ldots, n$.

(5) Podle 3.4(5) lze každý polynom $a_0 + a_1 t + \cdots + a_n t^n$ z $\mathbb{R}_n[t]$, resp. z $\mathbb{C}_n[t]$ ztotožnit s jeho vektorem $n + 1$ koeficientů

$[a_0, a_1, \ldots, a_n]$, takže roli přirozené báze v $\mathbb{R}_n[t]$, resp. v $\mathbb{C}_n[t]$ hrají homogenní polynomy $t^0 \equiv 1, t^1, \ldots, t^n$ a platí tedy $\dim \mathbb{R}_n[t] = \dim \mathbb{C}_n[t] = n + 1$.

(6) Pokud I je nekonečná množina, pak prostory $(\mathbb{R}^I, \mathcal{L}_\mathbb{R})$ i $(\mathbb{C}^I, \mathcal{L}_\mathbb{C})$ mají nekonečnou dimenzi. Zejména tedy mají nekonečnou dimenzi také prostory posloupností $(\mathbb{R}^\mathbb{N}, \mathcal{L}_\mathbb{R})$ a $(\mathbb{C}^\mathbb{N}, \mathcal{L}_\mathbb{C})$ stejně jako prostory polynomů $\mathbb{R}[t]$ a $\mathbb{C}[z]$.

3.4. **LINEÁRNÍ ZOBRAZENÍ.**

DEFINICE 3.26.
Nechť $(V_1, \mathcal{L}_{\mathbb{F}})$ a $(V_2, \mathcal{L}_{\mathbb{F}})$ jsou dva vektorové prostory. Pak zobrazení $T : V_1 \to V_2$, které je homomorfizmem (definice 2.10) nazýváme **lineárním zobrazením (lineárním operátorem)** z vektorového prostoru $(V_1, \mathcal{L}_{\mathbb{F}})$ do vektorového prostoru $(V_2, \mathcal{L}_{\mathbb{F}})$ a píšeme $T : (V_1, \mathcal{L}_{\mathbb{F}}) \to (V_2, \mathcal{L}_{\mathbb{F}})$[4].
Speciálně lineární zobrazení $T : (V, \mathcal{L}_{\mathbb{F}}) \to (\mathbb{F}, \mathcal{L}_{\mathbb{F}})$ se nazývá **lineární funkcionál na** V (viz též 3.4(1)).
Lineární zobrazení se nazývá **izomorfizmem** vektorových prostorů $(V_1, \mathcal{L}_{\mathbb{F}})$ a $(V_2, \mathcal{L}_{\mathbb{F}})$, jestliže je bijekcí V_1 na V_2 (viz úvahu na konci poznámky 2.61). Je-li T pouze prosté lineární zobrazení, nazývá se **izomorfní vnoření** prostoru $(V_1, \mathcal{L}_{\mathbb{F}})$ do $(V_2, \mathcal{L}_{\mathbb{F}})$.
Existuje-li alespoň jeden izomorfizmus $(V_1, \mathcal{L}_{\mathbb{F}})$ na $(V_2, \mathcal{L}_{\mathbb{F}})$, říkáme, že vektorové prostory $(V_1, \mathcal{L}_{\mathbb{F}})$ a $(V_2, \mathcal{L}_{\mathbb{F}})$ jsou **izomorfní** a píšeme $(V_1, \mathcal{L}_{\mathbb{F}}) \simeq (V_2, \mathcal{L}_{\mathbb{F}})$ nebo jen stručně $V_1 \simeq V_2$. Existuje-li pouze izomorfní vnoření, píšeme $(V_1, \mathcal{L}_{\mathbb{F}}) \precsim (V_2, \mathcal{L}_{\mathbb{F}})$ nebo $V_1 \precsim V_2$.

VĚTA 3.27 (Důkaz: D.25)**.**
Nechť $(V_1, \mathcal{L}_{\mathbb{F}})$ a $(V_2, \mathcal{L}_{\mathbb{F}})$ jsou dva vektorové prostory. Pak zobrazení $T : V_1 \to V_2$ je lineární právě když má následující vlastnosti:

(1) $\boldsymbol{x}, \boldsymbol{y} \in V_1 \Rightarrow T(\boldsymbol{x} + \boldsymbol{y}) = T(\boldsymbol{x}) + T(\boldsymbol{y})$
(vlastnost zachování grupového sečítání)
(2) $\boldsymbol{x} \in V_1, \alpha \in \mathbb{F} \Rightarrow T(\alpha \boldsymbol{x}) = \alpha T(\boldsymbol{x})$
(vlastnost zachování skalárního násobení).

Je-li T izomorfizmus, pak T^{-1} je rovněž lineární zobrazení (a tedy izomorfizmus) z $(V_2, \mathcal{L}_{\mathbb{F}})$ na $(V_1, \mathcal{L}_{\mathbb{F}})$. Zřejmě složení dvou lineárních zobrazení je rovněž lineární zobrazení.

DŮSLEDEK 3.28 (Důkaz D.26)**.**
Každé lineární zobrazení $T : (V_1, \mathcal{L}_{\mathbb{F}}) \to (V_2, \mathcal{L}_{\mathbb{F}})$ zachovává libovolné

[4]místo $\boldsymbol{y} = T(\boldsymbol{x})$ píšeme stručněji také $\boldsymbol{y} = T\boldsymbol{x}$

lineární kombinace vektorů, tj. pro $\alpha_i \in \mathbb{F}$ a $\boldsymbol{x}_i \in V_1$, $i = 1, \dots, n$, platí: $T(\alpha_1 \boldsymbol{x}_1 + \cdots + \alpha_n \boldsymbol{x}_n) = \alpha_1 T(\boldsymbol{x}_1) + \cdots + \alpha_n T(\boldsymbol{x}_n)$.

VĚTA 3.29 (Důkaz D.27).
Nechť $T : (V_1, \mathcal{L}_{\mathbb{F}}) \to (V_2, \mathcal{L}_{\mathbb{F}})$ *je lineární operátor, pak* $\mathcal{N}(T) := \{\boldsymbol{x} \in V_1 \mid T\boldsymbol{x} = \boldsymbol{0}\}$ *je vektorový podprostor v* $(V_1, \mathcal{L}_{\mathbb{F}})$ *nazývaný* **jádro (nulový podprostor) operátoru** T. *Podobně* $\mathcal{R}(T) := \{\boldsymbol{y} \in V_2 \mid \exists\, \boldsymbol{x} \in V_1 : \boldsymbol{y} = T\boldsymbol{x}\}$ *je vektorový podprostor ve* $(V_2, \mathcal{L}_{\mathbb{F}})$ *nazývaný* **obor hodnot operátoru** T.

DŮSLEDEK 3.30 (Důkaz D.28).
Nechť $T : (V_1, \mathcal{L}_{\mathbb{F}}) \to (V_2, \mathcal{L}_{\mathbb{F}})$ *je lineární operátor. Pak*

(1) *T je izomorfní vnoření právě když* $\mathcal{N}(T) = \{\boldsymbol{0}\}$.
(2) *T je izomorfizmus právě když* $\mathcal{N}(T) = \{\boldsymbol{0}\}$ *a* $\mathcal{R}(T) = V_2$.
(3) *T je izomorfní vnoření právě když obraz každé neprázdné konečné množiny lineárně nezávislé ve V_1 je také lineárně nezávislá množina ve V_2 s týmž počtem prvků.*
(4) *T je izomorfizmus právě když obraz nějaké báze ve V_1 je také báze ve V_2 téže mohutnosti. V takovém případě dokonce každá báze ve V_1 se zobrazí na bázi ve V_2.*

DEFINICE 3.31. Nechť $(V, \mathcal{L}_{\mathbb{F}})$ je n-rozměrný vektorový prostor a $E := \{\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\}$ jeho báze. Definujme zobrazení $[\cdot]_E : V \to \mathbb{F}^n$, které každému vektoru $\boldsymbol{x} \in V$ přiřazuje **vektor jeho souřadnic v bázi** E, tj. $[\boldsymbol{x}]_E := [\xi_1, \dots, \xi_n]$ je ona dle 3.17(3) jednoznačně určená n-tice skalárů taková, že $\boldsymbol{x} = \xi_1 \boldsymbol{e}_1 + \cdots + \xi_n \boldsymbol{e}_n$. Pokud báze E ve V bude pevně dána, budeme též psát stručně $[\boldsymbol{x}]$ místo $[\boldsymbol{x}]_E$.

VĚTA 3.32 (Důkaz D.29).
Zobrazení $[\cdot]_E : V \to \mathbb{F}^n$ *z předchozí definice je izomorfizmus vektorového prostoru* $(V, \mathcal{L}_{\mathbb{F}})$ *na* $(\mathbb{F}^n, \mathcal{L}_{\mathbb{F}})$.

DŮSLEDEK 3.33 (Důkaz D.30).

(1) *Dva konečně rozměrné vektorové prostory V_1 a V_2 nad týmž polem $\mathbb{F}$ mají stejnou dimenzi právě když* $(V_1, \mathcal{L}_{\mathbb{F}}) \simeq (V_2, \mathcal{L}_{\mathbb{F}})$.

(2) *Pro dva konečně rozměrné vektorové prostory* $(V_1, \mathcal{L}_\mathbb{F})$*,* $(V_2, \mathcal{L}_\mathbb{F})$ *platí* $\dim V_1 \leq \dim V_2$ *právě když* $(V_1, \mathcal{L}_\mathbb{F}) \precsim (V_2, \mathcal{L}_\mathbb{F})$*.*

POZNÁMKA 3.34.
Každý lineární operátor $T : (V_1, \mathcal{L}_\mathbb{F}) \to (V_2, \mathcal{L}_\mathbb{F})$, $V_1 = \mathcal{L}(E_1)$, je dle 3.28 jednoznačně určen jen svými hodnotami $T(E_1) = \{T\boldsymbol{e}\}_{e \in E_1}$ na generátorech $\boldsymbol{e} \in E_1$. Je-li $\boldsymbol{x} \in V_1$ libovolný vektor a $\boldsymbol{x} = \xi_1 \boldsymbol{e}_1 + \cdots + \xi_n \boldsymbol{e}_n$ nějaké jeho vyjádření jako lineární kombinace generátorů $e_i \in E_1, i = 1, \ldots, n$ (viz 3.13), pak totiž $T\boldsymbol{x} = \xi_1 T(\boldsymbol{e}_1) + \cdots + \xi_n T(\boldsymbol{e}_n)$ dle 3.28. Poznamenejme, že zatímco toto vyjádření nemusí být jediné možné (je tomu tak jen když E_1 je báze), obraz $T\boldsymbol{x}$ je vždy jediný bez ohledu na volbu tohoto vyjádření.

DEFINICE 3.35.
Nechť $T : (V_1, \mathcal{L}_\mathbb{F}) \to (V_2, \mathcal{L}_\mathbb{F})$ je lineární operátor, E_1 n-prvková báze ve V_1 a E_2 m-prvková báze ve V_2. Pak dle předchozí poznámky a s ohledem na 3.32 je T jednoznačně určen vektory souřadnic $[T\boldsymbol{e}]_{E_2}$ pro $\boldsymbol{e} \in E_1$. Systém n vektorů (každý délky m) značený $[T]_{E_1,E_2} := \{[T\boldsymbol{e}]_{E_2}\}_{e \in E_1}$ pak nazýváme **souřadnicovou reprezentací operátoru T v bázích E_1 a E_2**. Jsou-li obě báze pevně dány, píšeme opět stručně $[T]$ místo $[T]_{E_1,E_2}$.

VĚTA 3.36 (Důkaz D.31)**.**
Nechť $T : (V_1, \mathcal{L}_\mathbb{F}) \to (V_2, \mathcal{L}_\mathbb{F})$ *je lineární operátor,* $V_1 = \mathcal{L}(E_1)$*. Pak platí:*

(1) $T(E_1)$ *generuje* $\mathcal{R}(T)$*.*
(2) $T(E_1)$ *generuje* V_2 *právě když* T *je surjekce.*
(3) *Je-li* T *izomorfní vnoření a* E_1 *báze, pak* $T(E_1)$ *je báze v* $\mathcal{R}(T)$*.*
(4) *Je-li* T *izomorfní vnoření a* E_1 *báze, pak* $T(E_1)$ *je lineárně nezávislá podmnožina ve* V_2*.*
(5) *Je-li* T *izomorfizmus a* E_1 *báze, pak* $T(E_1)$ *je báze ve* V_2*.*
(6) *Každé zobrazení* f *báze* E_1 *do prostoru* V_2 *se dá jednoznačně rozšířit na lineární operátor* V_1 *do* V_2*. Je-li* f *prosté zobrazení do nějaké báze* E_2 *ve* V_2 *(resp. bijekce na* E_2*), pak toto rozšíření je izomorfní vnoření (resp. izomorfizmus).*

<u>PŘÍKLAD</u> 3.37. Uvážíme-li 3.25(5), pak zobrazení $\varphi(a_0 + a_1 t + \cdots + a_n t^n) := [a_0, a_1, \ldots, a_n]$ definuje izomorfizmus z $(\mathbb{R}_n[t], \mathcal{L}_\mathbb{R})$ na $(\mathbb{R}^{n+1}, \mathcal{L}_\mathbb{R})$, resp. z $(\mathbb{C}_n[z], \mathcal{L}_\mathbb{C})$ na $(\mathbb{C}^{n+1}, \mathcal{L}_\mathbb{C})$. Analogicky $\psi(a_0 + a_1 t + \cdots + a_n t^n) := \{a_0, a_1, \ldots, a_n, 0, \ldots\}$ definuje izomorfní vnoření z $(\mathbb{R}_n[t], \mathcal{L}_\mathbb{R})$ do $(\mathbb{R}^\mathbb{N}, \mathcal{L}_\mathbb{R})$, resp. z $(\mathbb{C}_n[t], \mathcal{L}_\mathbb{C})$ do $(\mathbb{C}^\mathbb{N}, \mathcal{L}_\mathbb{C})$.

VĚTA 3.38.
Nechť $(V_1, \mathcal{L}_\mathbb{F})$ a $(V_2, \mathcal{L}_\mathbb{F})$ jsou dva vektorové prostory. Nechť $\mathcal{L}(V_1, V_2)$ značí množinu všech lineárních operátorů z V_1 do V_2 s operacemi z $\mathcal{L}_\mathbb{F}$ definovanými po složkách jako v 3.4(4), tj. pro $T, T_1, T_2 \in \mathcal{L}(V_1, V_2)$ a každé $\boldsymbol{x} \in V_1$ klademe:
$(T_1 + T_2)(\boldsymbol{x}) := T_1(\boldsymbol{x}) + T_2(\boldsymbol{x}), \quad (-T)(\boldsymbol{x}) := -T(\boldsymbol{x}),$
$T \equiv 0 \;\Leftrightarrow\; T(\boldsymbol{x}) = 0, \quad (\alpha T)(\boldsymbol{x}) := \alpha T(\boldsymbol{x}).$
Pak $\mathcal{L}(V_1, V_2)$ je vektorový prostor nad $\mathbb{F}$.

Důkaz. Zřejmý: axiomy (L1)–(L4) prostoru $(V_2, \mathcal{L}_\mathbb{F})$ se po složkách přenesou na $\mathcal{L}(V_1, V_2)$. $\square$

3.5. FAKTOR PROSTORY A PŘÍMÝ SOUČET.

Věta 3.39.
Nechť $(V, \mathcal{L}_{\mathbb{F}})$ *je vektorový prostor a* $\sim$ *nějaká relace ekvivalence na* V *a* $\overline{V} := V/\!\sim$ *příslušný rozklad na* V*. Pak relace* $\sim$ *je kongruence na* $(V, \mathcal{L}_{\mathbb{F}})$ *ve smyslu definice 2.42 právě když pro* $\boldsymbol{x}, \boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}', \boldsymbol{x}'_1, \boldsymbol{x}'_2 \in V$ *platí implikace:*

(1) $\boldsymbol{x}_1 \sim \boldsymbol{x}'_1, \boldsymbol{x}_2 \sim \boldsymbol{x}'_2 \Rightarrow \boldsymbol{x}_1 + \boldsymbol{x}_2 \sim \boldsymbol{x}'_1 + \boldsymbol{x}'_2$,
(2) $\alpha \in \mathbb{F}$, $\boldsymbol{x} \sim \boldsymbol{x}' \Rightarrow \alpha\boldsymbol{x} \sim \alpha\boldsymbol{x}'$.

V takovém případě třída $\overline{\mathbf{0}} \in \overline{V}$ *obsahující nulový prvek je vektorovým podprostorem ve* V*.*

Důsledek 3.40.
Každý vektorový podprostor W *vektorového prostoru* $(V, \mathcal{L}_{\mathbb{F}})$ *určuje kongruenci* $\overset{W}{\sim}$ *na* V *s vlastností* $W = \overline{\mathbf{0}}$ *a naopak dle 3.39. Příslušný faktor prostor* $(\overline{V}, \mathcal{L}_{\mathbb{F}})$ *tvořený odpovídajícími třídami rozkladu pak značíme jako* V/W *a nazýváme jej* **faktor prostorem** V **modulo (podle)** W*. Každá jeho třída obsahující vektor* $\boldsymbol{x}$ *je jednoznačně určena podprostorem* W *ve tvaru* $\overline{\boldsymbol{x}} = \{\boldsymbol{x} + \boldsymbol{w} \mid \boldsymbol{w} \in W\}$*. Místo* $\overline{\boldsymbol{x}}$ *pak píšeme* $\boldsymbol{x} + W$*. Zejména samotný podprostor* $W = \mathbf{0} + W$ *tvoří třídu obsahující nulový vektor* $\mathbf{0}$*.*
Přitom platí $\boldsymbol{x} \overset{W}{\sim} \boldsymbol{y} \;\Leftrightarrow\; \boldsymbol{y} - \boldsymbol{x} \in W$*. V takovém případě říkáme, že vektory* $\boldsymbol{x}$ *a* $\boldsymbol{y}$ *jsou* **kongruentní modulo** W*.*
Pro příslušné kanonické lineární zobrazení $V \to V/W$ *z věty 2.43,* $\boldsymbol{x} \mapsto \boldsymbol{x} + W$*, pak tedy platí:*
$(\boldsymbol{x}+\boldsymbol{y})+W = (\boldsymbol{x}+W)+(\boldsymbol{y}+W)$, $(-\boldsymbol{x})+W = -(\boldsymbol{x}+W)$, $\mathbf{0} \mapsto W$, $(\alpha\boldsymbol{x}) + W = \alpha(\boldsymbol{x}+W)$ *pro každé* $\alpha \in \mathbb{F}$.

Důsledek 3.41.
Je-li $T : (V_1, \mathcal{L}_{\mathbb{F}}) \to (V_2, \mathcal{L}_{\mathbb{F}})$ *lineární zobrazení a* $V_1/\overset{T}{\sim}$ *příslušný kanonický rozklad dle definice 2.40, pak* $V_1/\overset{T}{\sim} \;=\; V_1/\mathcal{N}(T)$.

<u>*Poznámka*</u> 3.42.
Podobně každá faktor grupa V/W grupy $(V, +, 0)$ je určena nějakou

podgrupou W ve V. Stačí vlastnost (2) ve větě 3.39 nahradit vlastností: $\boldsymbol{x} \sim \boldsymbol{x}' \Rightarrow -\boldsymbol{x} \sim -\boldsymbol{x}'$.
Příkladem je grupa $(\mathbb{Z}_N, \oplus, 0)$, která je izomorfní s faktor grupou grupy $(\mathbb{Z}, +, 0)$ podle podgrupy $N\mathbb{Z} := \{Nk \,|\, k \in \mathbb{Z}\}$. Píšeme pak $\mathbb{Z}_N \simeq \mathbb{Z}/N\mathbb{Z}$. Pak

$$a \overset{N\mathbb{Z}}{\sim} b \;\Leftrightarrow\; b-a \in N\mathbb{Z} \;\Leftrightarrow\; b-a = Nk \text{ pro nějaké } k \in \mathbb{Z} \;\Leftrightarrow\; N|(b-a),$$

což přesně odpovídá kongruenci z příkladu 2.62(2).

DEFINICE 3.43.
Nechť $\{(W_i, \mathcal{L}_\mathbb{F})\}_{i\in I}$ je systém vektorových podprostorů vektorového prostoru $(V, \mathcal{L}_\mathbb{F})$. Pak podprostor $W := \mathcal{L}(\bigcup_{i\in I} W_i)$ nazýváme **součtem vektorových podprostorů** W_i**,** $i \in I$ a píšeme $W = \sum_{i\in I} W_i$.
Jestliže navíc platí $W_i \cap \mathcal{L}(\bigcup_{j\in I, j\neq i} W_j) = \{\boldsymbol{0}\}$ pro každé $i \in I$, pak součet nazýváme **přímým součtem vektorových podprostorů** W_i**,** $i \in I$ a píšeme $W = \dot{\sum}_{i\in I} W_i$.
Speciálně v případě součtu dvou, resp. konečného počtu ($n \geq 2$) podprostorů píšeme $W = W_1 + W_2$, resp. $W = W_1 + \cdots + W_n$. Podobně v případě přímého součtu dvou[5], resp. konečného počtu ($n \geq 2$) podprostorů píšeme $W = W_1 \dotplus W_2$, resp. $W = W_1 \dotplus \cdots \dotplus W_n$.

<u>*Poznámka*</u> 3.44.
Součet ani přímý součet podprostorů zřejmě nezávisí na pořadí a uzávorkování sčítanců a jsou to tedy komutativní a asociativní operace.

VĚTA 3.45. *Pro podprostory z předchozí definice platí:*

(1) $W = \sum_{i\in I} W_i$ *právě když*
$W = \{\boldsymbol{x} \in V \,|\, \boldsymbol{x} = \sum_{j\in J} \boldsymbol{x}_j, \boldsymbol{x}_j \in W_j, J \subseteq I, \operatorname{card} J < \infty\}$.
(2) $W = W_1 + \cdots + W_n$ *právě když*
$W = \{\boldsymbol{x}_1 + \cdots + \boldsymbol{x}_n \,|\, \boldsymbol{x}_i \in W_i, i = 1, \ldots, n\}$.
(3) $W = \dot{\sum}_{i\in I} W_i$ *právě když*
$W = \{\boldsymbol{x} \in V \,|\, \boldsymbol{x} = \sum_{j\in J} \boldsymbol{x}_j, \boldsymbol{x}_j \in W_j, J \subseteq I, \operatorname{card} J < \infty\}$,

[5]dodatečná podmínka je v tomto případě tvaru $W_1 \cap W_2 = \{\boldsymbol{0}\}$.

kde vyjádření každého vektoru $\boldsymbol{x} \in W$ ve tvaru součtu $\boldsymbol{x} = \sum_{j \in J} \boldsymbol{x}_j$ je jediné až na pořadí a počet nulových sčítanců $\boldsymbol{x}_j$.

(4) *$W = W_1 \dotplus \cdots \dotplus W_n$ právě když $W = \{\boldsymbol{x}_1 + \cdots + \boldsymbol{x}_n \mid \boldsymbol{x}_i \in W_i, i = 1, \ldots, n\}$, kde vyjádření $\boldsymbol{x}_1 + \cdots + \boldsymbol{x}_n$ každého vektoru je až na pořadí sčítanců jediné.*

DŮSLEDEK 3.46.
$W = W_1 \dotplus \cdots \dotplus W_n$ právě když $W \simeq W_1 \times \cdots \times W_n$.

VĚTA 3.47 ([`Šik:V3.43 s.32`]).
Ke každému podprostoru W vektorového prostoru $(V, \mathcal{L}_{\mathbb{F}})$ existuje (obecně ne jediný) podprostor W' ve V tak, že $V = W \dotplus W'$ a $\dim V = \dim W + \dim W'$. Podprostor W' se nazývá **přímý doplněk** *W* **ve** *V.*

Věta 3.48 ([`Šik:V3.44 s.33`]).
Nechť $(V, \mathcal{L}_{\mathbb{F}})$ je vektorový prostor a $V = W_1 \dotplus W_2$, pak $V/W_1 \simeq W_2$ a každá třída rozkladu V/W_1 obsahuje právě jeden prvek z W_2 (podobně po záměně role W_1 a W_2).

VĚTA 3.49 ([`Šik:V3.45 s.33`]).
Nechť $(V, \mathcal{L}_{\mathbb{F}})$ je vektorový prostor a $V = W_1 \dotplus W_2$, pak $\dim V = \dim(W_1 + W_2) = \dim W_1 + \dim W_2$.

VĚTA 3.50 ([`Šik:V3.46 s.33`]).
Nechť $(V, \mathcal{L}_{\mathbb{F}})$ je vektorový prostor a W_1 a W_2 jeho podprostory, pak $\dim(W_1 \cap W_2) + \dim(W_1 + W_2) = \dim W_1 + \dim W_2$.

PŘÍKLAD 3.51.

(1) Nechť $\mathbf{0} \neq \boldsymbol{u} \in \mathbb{R}^2$ je nějaký vektor, pak $W := \mathcal{L}(\{\boldsymbol{u}\}) = \{\xi \boldsymbol{u} \mid \xi \in \mathbb{R}\}$ je jednorozměrný vektorový podprostor v $(\mathbb{R}^2, \mathcal{L}_{\mathbb{R}})$ generovaný vektorem $\boldsymbol{u}$. Tento podprostor je v Euklidovské rovině s pevně zvoleným počátkem reprezentován přímkou procházející tímto počátkem ve směru vektoru $\boldsymbol{u}$. Pak rozklad $\mathbb{R}^2/W$ dle 3.40 je tvořen všemi přímkami rovnoběžnými s W.

(2) Nechť W_1 a W_2 jsou dva různé jednorozměrné vektorové podprostory jako v (1) reprezentované dvěma přímkami procházejícími počátkem v různých směrech $\boldsymbol{u}_1$ a $\boldsymbol{u}_2$. Pak $\mathbb{R}^2 = W_1 \dot{+} W_2$, neboť $W_1 \cap W_2 = \{[0,0]\}$ a $\mathbb{R}^2 = \mathcal{L}(W_1 \cup W_2) = \mathcal{L}(\{\boldsymbol{u}_1, \boldsymbol{u}_2\})$, neboť $\boldsymbol{u}_1, \boldsymbol{u}_2$ jsou zřejmě nezávislé a tudíž tvoří bázi v $\mathbb{R}^2$. Dle 3.49 podle očekávání platí $2 = \dim \mathbb{R}^2 = \dim W_1 + \dim W_2 = 1 + 1$.

(3) Nechť W_1 a W_2 jsou dva různé dvourozměrné podprostory v $(\mathbb{R}^3, \mathcal{L}_{\mathbb{R}})$ reprezentované různými rovinami procházejícími počátkem Eukleidovského prostoru $\mathbb{R}^3$. Zřejmě $\mathbb{R}^3 = W_1 + W_2$ a dle 3.50 platí $\dim(W_1 \cap W_2) = \dim W_1 + \dim W_2 - \dim \mathbb{R}^3 = 2 + 2 - 3 = 1$. Podle očekávání je tedy průnikem těchto rovin nějaká přímka procházející počátkem a součet $\mathbb{R}^3 = W_1 + W_2$ tedy nemůže být přímým součtem. Toho lze dosáhnout jen když W_1 je přímka a W_2 rovina (nebo naopak), kdy $\dim(W_1 \cap W_2) = 1 + 2 - 3 = 0$, tj. $W_1 \cap W_2 = \{[0,0,0]\}$.

DEFINICE 3.52. Nechť W je vektorový podprostor vektorového prostoru $(V, \mathcal{L}_{\mathbb{F}})$ a $P : V \twoheadrightarrow W$ lineární operátor s vlastností: $P\boldsymbol{x} = \boldsymbol{x}$ pro každé $\boldsymbol{x} \in W$. Pak P se nazývá **projekční**. P je zřejmě surjektivní a $P^2 = P$, tj. $P(P\boldsymbol{x}) = P\boldsymbol{x}$ pro každé $\boldsymbol{x} \in V$ (tzv. vlastnost **idempotence**).

VĚTA 3.53. *Nechť $(V, \mathcal{L}_{\mathbb{F}})$ je vektorový prostor a $V = W_1 \dot{+} W_2$. Definujme zobrazení $P_1 : V \to W_1$ takto: $P_1(\boldsymbol{x}) := \boldsymbol{x}_1$ je onen dle věty 3.45(4) jednoznačně určený prvek z vyjádření $\boldsymbol{x} = \boldsymbol{x}_1 + \boldsymbol{x}_2$, $\boldsymbol{x}_1 \in W_1$, $\boldsymbol{x}_2 \in W_2$. Pak P_1 je projekční operátor nazývaný* **operátorem rovnoběžné**[6] **projekce na podprostor** *W_1, přičemž $\mathcal{N}(P_1) = W_2$ a $V/\overset{P_1}{\sim} = V/W_2$.*

[6]rozumí se rovnoběžně s podprostorem W_2

3.6. PROSTORY S NORMOU A SKALÁRNÍM SOUČINEM.

Všude v tomto odstavci uvažujeme pouze reálné nebo komplexní vektorové prostory, tj. $\mathbb{F} \subseteq \mathbb{C}$, zpravidla $\mathbb{F} = \mathbb{R}$ nebo $\mathbb{F} = \mathbb{C}$.

DEFINICE 3.54. Nechť V je (reálný nebo komplexní) vektorový prostor. **Normou na** V rozumíme funkci[7] $\|\cdot\| : V \to \mathbb{R}^+$ s těmito vlastnostmi:

(N1) $\|\boldsymbol{x}+\boldsymbol{y}\| \leq \|\boldsymbol{x}\| + \|\boldsymbol{y}\|$ pro každé $\boldsymbol{x}, \boldsymbol{y} \in V$ (trojúhelníková nerovnost).
(N2) $\|\alpha\boldsymbol{x}\| = |\alpha|\,\|\boldsymbol{x}\|$ pro každé $\boldsymbol{x} \in V$ a $\alpha \in \mathbb{F}$.
(N3) Pro každé $\boldsymbol{x} \in V$ platí $\|\boldsymbol{x}\| \geq 0$, přičemž $\|\boldsymbol{x}\| = 0 \;\Leftrightarrow\; \boldsymbol{x} = \boldsymbol{0}$.

Vektorový prostor V pak nazýváme **normovaným lineárním (vektorovým) prostorem**, zkráceně **NL-prostorem** a píšeme $(V, \mathcal{L}_{\mathbb{F}}, \|\cdot\|)$.

VĚTA 3.55. *Vlastnosti normy, důkaz D.32*
Z axiomů (N1) až (N3) bezprostředně vyplývají některé další užitečné vlastnosti normy, například:

(N4) $|\,\|\boldsymbol{x}\| - \|\boldsymbol{y}\|\,| \leq \|\boldsymbol{x} \pm \boldsymbol{y}\| \leq \|\boldsymbol{x}\| + \|\boldsymbol{y}\|$ *pro každé* $\boldsymbol{x}, \boldsymbol{y} \in V$.

PŘÍKLAD 3.56.

(1) Absolutní hodnota $|\cdot|$ je normou v $(\mathbb{F}, \mathcal{L}_{\mathbb{F}})$.
(2) Podobně pro $\boldsymbol{x} =: [x_1, \ldots, x_n] \in \mathbb{F}^n$, $n \in \mathbb{N}$, definuje vztah $\|\boldsymbol{x}\|_1 := |x_1| + \cdots + |x_n|$ tzv. **1-normu v** $(\mathbb{F}^n, \mathcal{L}_{\mathbb{F}})$.
(3) Dá se ukázat, že pro libovolné $p \in \mathbb{N}$ je rovněž $\|\boldsymbol{x}\|_p := \sqrt[p]{|x_1|^p + \cdots + |x_n|^p}$ tzv. **p-norma v** $(\mathbb{F}^n, \mathcal{L}_{\mathbb{F}})$. V limitě pro $p \to \infty$ dostaneme normu $\|\boldsymbol{x}\|_\infty := \max(|x_1|, \ldots, |x_n|)$.

POZNÁMKA 3.57. Norma představuje míru pro velikost vektorů ve vektorovém prostoru. Norma $\|\boldsymbol{x}\|_2$ z předchozího příkladu je běžně užívaná **Euklidovská norma**.

---

[7]někdy také budeme psát $\|\cdot\|_V$ místo $\|\cdot\|$, abychom zdůraznili příslušnost normy k prostoru V.

DEFINICE 3.58. Nechť V je (reálný nebo komplexní) vektorový prostor. **Skalárním (vnitřním) součinem na** V rozumíme funkci[8] $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{F}$ s těmito vlastnostmi:

(S1) $\langle \boldsymbol{x} + \boldsymbol{y}, \boldsymbol{z} \rangle = \langle \boldsymbol{x}, \boldsymbol{z} \rangle + \langle \boldsymbol{y}, \boldsymbol{z} \rangle$ pro každé $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in V$.
(S2) $\langle \alpha \boldsymbol{x}, \boldsymbol{y} \rangle = \alpha \langle \boldsymbol{x}, \boldsymbol{y} \rangle$ pro každé $\boldsymbol{x}, \boldsymbol{y} \in V$ a $\alpha \in \mathbb{F}$.
(S3) $\langle \boldsymbol{y}, \boldsymbol{x} \rangle = \overline{\langle \boldsymbol{x}, \boldsymbol{y} \rangle}$ pro každé $\boldsymbol{x}, \boldsymbol{y} \in V$, zejména tedy $\langle \boldsymbol{x}, \boldsymbol{x} \rangle \in \mathbb{R}$.
(S4) Pro každé $\boldsymbol{x} \in V$ platí $\langle \boldsymbol{x}, \boldsymbol{x} \rangle \geq 0$, přičemž $\langle \boldsymbol{x}, \boldsymbol{x} \rangle = 0 \Leftrightarrow \boldsymbol{x} = \boldsymbol{0}$.

Vektorový prostor V pak nazýváme **lineárním (vektorovým) prostorem s vnitřním součinem**, zkráceně **VS-prostorem** a píšeme $(V, \mathcal{L}_{\mathbb{F}}, \langle \cdot, \cdot \rangle)$.

VĚTA 3.59. *(Vlastnosti skalárního součinu, důkaz D.33)*
Z axiomů (S1) až (S4) vyplývají některé další užitečné vlastnosti skalárního součinu, například:

(S5) $\langle \boldsymbol{x}, \boldsymbol{y} + \boldsymbol{z} \rangle = \langle \boldsymbol{x}, \boldsymbol{y} \rangle + \langle \boldsymbol{x}, \boldsymbol{z} \rangle$ *pro každé* $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in V$.
(S6) $\langle \boldsymbol{x}, \alpha \boldsymbol{y} \rangle = \overline{\alpha} \langle \boldsymbol{x}, \boldsymbol{y} \rangle$ *pro každé* $\boldsymbol{x}, \boldsymbol{y} \in V$ *a* $\alpha \in \mathbb{F}$.
(S7) $\langle \boldsymbol{0}, \boldsymbol{x} \rangle = \langle \boldsymbol{x}, \boldsymbol{0} \rangle = 0$ *pro každé* $\boldsymbol{x} \in V$.

POZNÁMKA 3.60.
Je-li V reálný vektorový prostor ($\mathbb{F} = \mathbb{R}$), pak (S3) a (S6) jsou tvaru:

(S3') $\langle \boldsymbol{y}, \boldsymbol{x} \rangle = \langle \boldsymbol{x}, \boldsymbol{y} \rangle$ pro každé $\boldsymbol{x}, \boldsymbol{y} \in V$ (symetrie).
(S6') $\langle \boldsymbol{x}, \alpha \boldsymbol{y} \rangle = \alpha \langle \boldsymbol{x}, \boldsymbol{y} \rangle$ pro každé $\boldsymbol{x}, \boldsymbol{y} \in V$ a $\alpha \in \mathbb{R}$.

Vlastnosti (S1), (S2), (S5) a (S6'), resp. (S6), znamenají, že $\langle \cdot, \cdot \rangle$ je tzv. **bilineární forma na V**. Vlastnost (S3') znamená, že $\langle \cdot, \cdot \rangle$ je dokonce **symetrická** bilineární forma.
Vzhledem k vlastnostem bilinearity můžeme dále s výhodou provádět

[8] někdy také budeme psát $\langle \cdot, \cdot \rangle_V$ místo $\langle \cdot, \cdot \rangle$, abychom zdůraznili příslušnost skalárního součinu k prostoru V.

následující úpravy ($\xi_i, \eta_j \in \mathbb{F},\ \boldsymbol{x}_i, \boldsymbol{y}_j \in V$):

$$\langle \sum_{i=1}^{n} \xi_i \boldsymbol{x}_i, \sum_{j=1}^{m} \eta_j \boldsymbol{y}_j \rangle = \sum_{i=1}^{n} \xi_i \langle \boldsymbol{x}_i, \sum_{j=1}^{m} \eta_j \boldsymbol{y}_j \rangle = \sum_{i=1}^{n} \xi_i \sum_{j=1}^{m} \overline{\eta}_j \langle \boldsymbol{x}_i, \boldsymbol{y}_j \rangle =$$
$$= \sum_{i=1}^{n} \sum_{j=1}^{m} \xi_i \overline{\eta}_j \langle \boldsymbol{x}_i, \boldsymbol{y}_j \rangle. \tag{3.1}$$

<u>**VĚTA**</u> **3.61** ((Cauchy-)Schwarzova nerovnost, důkaz D.34)**.**
`[KaSk:V11.5 s.105]`

(S8) $|\langle \boldsymbol{x}, \boldsymbol{y} \rangle| \leq \sqrt{\langle \boldsymbol{x}, \boldsymbol{x} \rangle} \sqrt{\langle \boldsymbol{y}, \boldsymbol{y} \rangle} \overset{(S9)}{=} \|\boldsymbol{x}\| \, \|\boldsymbol{y}\|$ *pro každé* $\boldsymbol{x}, \boldsymbol{y} \in V$, *přičemž rovnost nastane jen v případě, že* $\boldsymbol{x}, \boldsymbol{y}$ *jsou lineárně závislé, tj. jen když jeden z nich je skalárním násobkem druhého (viz větu 3.18).*

<u>**DŮSLEDEK**</u> **3.62** (Důkaz D.35)**.**

(S9) $\|\boldsymbol{x}\| := \sqrt{\langle \boldsymbol{x}, \boldsymbol{x} \rangle}$ *je norma na* V *nazývaná* **normou odvozenou ze skalárního součinu** $\langle \cdot, \cdot \rangle$ *nebo také* **normou indukovanou skalárním součinem** $\langle \cdot, \cdot \rangle$.

Věta 3.63 (Důkaz D.36)**.**
V NL-prostoru V *s normou* $\|\cdot\|$ *lze zavést vnitřní součin* $\langle \cdot, \cdot \rangle$ *indukující tuto normu dle (S9) právě když platí tzv.* **rovnoběžníkový zákon** *(součet délek úhlopříček rovnoběžníku=součet délek stran):*

(S10) $\|\boldsymbol{x} + \boldsymbol{y}\|^2 + \|\boldsymbol{x} - \boldsymbol{y}\|^2 = 2(\|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2)$ *pro každé* $\boldsymbol{x}, \boldsymbol{y} \in V$.

<u>**PŘÍKLAD**</u> **3.64.**
- $(\mathbb{C}^n, \mathcal{L}_{\mathbb{C}})$, $n \in \mathbb{N}$, je VS-prostorem s vnitřním součinem $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \sum_{i=1}^{n} x_i \overline{y}_i$.
- $(\mathbb{R}^n, \mathcal{L}_{\mathbb{R}})$, $n \in \mathbb{N}$, je VS-prostorem s vnitřním součinem $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \sum_{i=1}^{n} x_i y_i$.
- Indukovanou normou je v obou případech euklidovská norma, neboť $\langle \boldsymbol{x}, \boldsymbol{x} \rangle = \sum_{i=1}^{n} x_i \overline{x}_i = \sum_{i=1}^{n} |x_i|^2 = \|\boldsymbol{x}\|_2^2$.
- Protože každé dva nenulové reálné vektory $\boldsymbol{x}, \boldsymbol{y}$ generují nejvýše

dvourozměrný podprostor v $(\mathbb{R}^n, \mathcal{L}_\mathbb{R})$, který je dle 3.32 izomorfní s $(\mathbb{R}^2, \mathcal{L}_\mathbb{R})$ můžeme bez újmy na obecnosti předpokládat, že $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^2$. Pak užitím Pythagorovy věty dostáváme (α a β jsou úhly, které po řadě vektory $\boldsymbol{x}$ a $\boldsymbol{y}$ svírají s osou x):

$$\begin{aligned}\langle \boldsymbol{x}, \boldsymbol{y} \rangle &= x_1 y_1 + x_2 y_2 = \\ &= (\|\boldsymbol{x}\| \cos\alpha)(\|\boldsymbol{y}\| \cos\beta) + (\|\boldsymbol{x}\| \sin\alpha)(\|\boldsymbol{y}\| \sin\beta) = \\ &= \|\boldsymbol{x}\|\,\|\boldsymbol{y}\|(\cos\alpha\cos\beta + \sin\alpha\sin\beta) = \\ &= \|\boldsymbol{x}\|\|\boldsymbol{y}\|\cos(\beta - \alpha).\end{aligned}$$

Pak $\varphi := \beta - \alpha$ je úhel mezi směrově orientovanými vektory $\boldsymbol{x}$ a $\boldsymbol{y}$ a můžeme psát:

$$-1 \leq \cos\varphi := \frac{\langle \boldsymbol{x}, \boldsymbol{y} \rangle}{\|\boldsymbol{x}\|\|\boldsymbol{y}\|} \leq 1,\ 0 \leq \varphi \leq \pi, \tag{3.2a}$$

což poskytuje geometrickou interpretaci Schwarzovy nerovnosti.
V komplexním případě je $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$ obecně komplexní číslo, takže úhel můžeme zavést jen jako úhel mezi neorientovanými vektory:

$$0 \leq \cos\varphi := \frac{|\langle \boldsymbol{x}, \boldsymbol{y} \rangle|}{\|\boldsymbol{x}\|\|\boldsymbol{y}\|} \leq 1,\ 0 \leq \varphi \leq \frac{\pi}{2}, \tag{3.2b}$$

Skalární součin tedy prostřednictvím Schwarzovy nerovnosti umožňuje zavést úhlovou geometrii do libovolného abstraktního vektorového prostoru se skalárním součinem dle následující definice.

DEFINICE 3.65.
Nechť V je reálný (resp. komplexní) vektorový prostor a $\boldsymbol{x}, \boldsymbol{y} \in V$ jeho dva nenulové vektory. Pak **úhlem mezi $\boldsymbol{x}$ a $\boldsymbol{y}$ (svíraným vektory $\boldsymbol{x}$ a $\boldsymbol{y}$)** rozumíme úhel φ určený svým kosinem dle (3.2a) (resp. dle (3.2b)). Je-li $\boldsymbol{x} = \mathbf{0}$ nebo $\boldsymbol{y} = \mathbf{0}$, klademe definitoricky $\varphi = \frac{\pi}{2}$.
• Řekneme, že vektory $\boldsymbol{x}$ a $\boldsymbol{y}$ jsou **ortogonální**, jestliže $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0$ (tj. když svírají pravý úhel), píšeme $\boldsymbol{x} \perp \boldsymbol{y}$. Zřejmě nulový vektor $\mathbf{0}$ je dle (S7) kolmý na každý vektor $\boldsymbol{x} \in V$ a dle (S4) je to současně jediný vektor, který je kolmý sám na sebe.
• Podobně podmnožiny $M, N \subseteq V$ se nazývají **k sobě ortogonální**,

jestliže $\boldsymbol{x} \perp \boldsymbol{y}$ pro každou dvojici $\boldsymbol{x} \in M$ a $\boldsymbol{y} \in N$. Píšeme opět $M \perp N$ (místo $\{\boldsymbol{x}\} \perp N$ píšeme stručně $\boldsymbol{x} \perp N$).

• Řekneme, že množina $M \subseteq V$ je **ortogonální**, jestliže $\boldsymbol{x} \perp \boldsymbol{y}$ pro každou dvojici $\boldsymbol{x}, \boldsymbol{y} \in M$, $\boldsymbol{x} \neq \boldsymbol{y}$. Ortogonální množina M se nazývá **ortonormální**[9], jestliže navíc $\|\boldsymbol{x}\| = 1$ pro každé $\boldsymbol{x} \in M$.

<u>VĚTA</u> 3.66 (Důkaz D.37). `[KaSk:V11.8 s.106]`
Nechť $E := \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ je ortogonální množina VS-prostoru V. Pak platí:

(a) *množina $\{\alpha_1\boldsymbol{e}_1, \ldots, \alpha_n\boldsymbol{e}_n\}$ je ortogonální pro libovolná čísla $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$,*
(b) *pokud E neobsahuje nulové vektory, pak E lze normalizovat: množina $\{\frac{1}{\|\boldsymbol{e}_1\|}\boldsymbol{e}_1, \ldots, \frac{1}{\|\boldsymbol{e}_n\|}\boldsymbol{e}_n\}$ je ortonormální.*

<u>VĚTA</u> 3.67 (Pythagorova věta, Důkaz D.38). `[KaSk:V11.9 s.106]`

(S11) $\|\boldsymbol{x} + \boldsymbol{y}\|^2 = \|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2$ *pro každé $\boldsymbol{x}, \boldsymbol{y} \in V$, $\boldsymbol{x} \perp \boldsymbol{y}$.*

Je-li $E = \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$, $n \in \mathbb{N}$, ortogonální množina vektorového prostoru V. Pak platí

(S11') $\|\boldsymbol{e}_1 + \boldsymbol{e}_2 + \cdots + \boldsymbol{e}_n\|^2 = \|\boldsymbol{e}_1\|^2 + \|\boldsymbol{e}_2\|^2 + \cdots + \|\boldsymbol{e}_n\|^2$.

<u>VĚTA</u> 3.68 (Důkaz D.39).
Nechť E je ortogonální množina VS-prostoru V neobsahující nulové prvky. Pak E je lineárně nezávislá. Zejména tedy každá ortonormální množina $E \subseteq V$ je lineárně nezávislá. Jestliže taková množina E generuje celý prostor V (viz 3.19(3)), nazývá se **ortogonální, resp. ortonormální báze** *prostoru V (zkráceně OB, resp. ONB).*

<u>DŮSLEDEK</u> 3.69 (Důkaz D.40).
Nechť E je ONB VS-prostoru V, pak každý vektor $\boldsymbol{x} \in V$ má jediné vyjádření ve tvaru $\boldsymbol{x} = \sum_{\boldsymbol{e} \in E} \langle \boldsymbol{x}, \boldsymbol{e} \rangle \boldsymbol{e}$, kde suma má nejvýše konečně mnoho nenulových sčítanců, neboť $\operatorname{card}\{\boldsymbol{e} \in E \mid \langle \boldsymbol{x}, \boldsymbol{e} \rangle \neq 0\} < \infty$.

---

[9] Na rozdíl od ortogonální množiny nemůže dle (N3) ortonormální množina obsahovat nulové prvky.

Je-li V konečně rozměrný a $E = \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$, pak $\boldsymbol{x}$ má v této bázi vektor souřadnic[10] $[\boldsymbol{x}]_E = [\langle \boldsymbol{x}, \boldsymbol{e}_1\rangle, \ldots, \langle \boldsymbol{x}, \boldsymbol{e}_n\rangle]$.

DŮSLEDEK 3.70 (Souřadnicové vyjádření skalárního součinu v ONB)**.**
Nechť E je ONB VS-prostoru V, $\boldsymbol{x}, \boldsymbol{y} \in V$, pak skalární součin lze vyjádřit ve tvaru $\langle \boldsymbol{x}, \boldsymbol{y}\rangle = \sum_{\boldsymbol{e}\in E} \langle \boldsymbol{x}, \boldsymbol{e}\rangle \overline{\langle \boldsymbol{y}, \boldsymbol{e}\rangle}$, kde suma má nejvýše konečně mnoho nenulových sčítanců. Zejména v případě $\boldsymbol{x} = \boldsymbol{y}$ platí $\|\boldsymbol{x}\| = \sqrt{\sum_{\boldsymbol{e}\in E} |\langle \boldsymbol{x}, \boldsymbol{e}\rangle|^2}$.
Je-li V konečně rozměrný a $E = \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$, pak $\langle \boldsymbol{x}, \boldsymbol{y}\rangle = \sum_{i=1}^n \xi_i \overline{\eta}_i$ a $\|\boldsymbol{x}\| = \sqrt{\sum_{i=1}^n |\xi_i|^2}$, kde $[\boldsymbol{x}]_E =: [\xi_1, \ldots, \xi_n]$, $[\boldsymbol{y}]_E =: [\eta_1, \ldots, \eta_n]$, $\xi_i = \langle \boldsymbol{x}, \boldsymbol{e}_i\rangle$ a $\eta_i = \langle \boldsymbol{y}, \boldsymbol{e}_i\rangle$ pro $i = 1, \ldots, n$.

Důkaz. D.41. □

Věta 3.71 (Důkaz D.42)**.**
Nechť $\emptyset \neq M \subseteq V$ je podmnožina VS-prostoru V. Pak množina $M^\perp := \{\boldsymbol{x} \in V \mid \boldsymbol{x} \perp M\}$ je vektorový podprostor ve V a platí $\mathcal{L}(M)^\perp = M^\perp$. Množina $M^\perp$ se nazývá **ortogonální doplněk (komplement) množiny** *M* **ve** *V. Přitom $M \subseteq N \Rightarrow N^\perp \subseteq M^\perp$.*

POZNÁMKA 3.72. Z předchozí věty vyplývá důležitý fakt: k tomu, aby nějaký vektor $\boldsymbol{x} \in V$ byl kolmý na nějaký podprostor W ve V stačí, aby byl kolmý na nějakou obvykle podstatně menší množinu jeho generátorů (konečná množina, pokud $\dim W < \infty$).

VĚTA 3.73 (Důkaz D.43)**.**
Nechť $\{(W_i, \mathcal{L}_{\mathbb{F}})\}_{i\in I}$ je systém navzájem kolmých VS–podprostorů VS-prostoru $(V, \mathcal{L}_{\mathbb{F}})$, $W_i \perp W_j$ pro $i \neq j$. Pak jejich součet $W := \sum_{i\in I} W_i$ je přímý a nazývá se **ortogonální součet podprostorů** *$\{W_i\}_{i\in I}$.*

Místo $W = \dot{\sum}_{i\in I} W_i$ v takovém případě píšeme $W = \bigoplus_{i\in I} W_i$. Speciálně v případě ortogonálního součtu dvou, resp. konečného počtu $(n \geq 2)$ podprostorů píšeme $W = W_1 \oplus W_2$, resp. $W = W_1 \oplus \cdots \oplus W_n$.

[10] viz definici 3.31

<u>VĚTA</u> 3.74 (Důkaz D.44)**.**
Nechť $(V, \mathcal{L}_{\mathbb{F}})$ *je VS-prostor a* $V = W \oplus W'$. *Pak* $W' = W^{\perp}$ *je jediný přímý doplněk ortogonální k* W. *V tomto případě operátor rovnoběžné projekce* V *na* W *zavedený ve větě 3.53 nazýváme* **operátorem ortogonální projekce** *a značíme jej* P_W. *Každý vektor* $\boldsymbol{x} \in V$ *lze pak jednoznačně rozložit na součet* $\boldsymbol{x} = \widehat{\boldsymbol{x}} + \boldsymbol{x}^{\perp}$, *kde* $\widehat{\boldsymbol{x}} := P_W \boldsymbol{x} \in W$ *je* **ortogonální projekce** $\boldsymbol{x}$ **na** W *a* $\boldsymbol{x}^{\perp} \in W^{\perp}$ *je jednoznačně určená reziduální složka vektoru* $\boldsymbol{x}$, $\boldsymbol{x}^{\perp} \perp W$.

<u>DŮSLEDEK</u> 3.75 (Důkaz D.45)**.**
$I - P_W$ *je operátor ortogonální projekce* V *na* $W^{\perp}$ *a platí* $W^{\perp\perp} = W$.

<u>VĚTA</u> 3.76 (Některé vlastnosti operátoru ortogonální projekce)**.**
Nechť W_1 *a* W_2 *jsou vektorové podprostory VS-prostoru* V *a* P_{W_1} *a* P_{W_2} *operátory ortogonální projekce prostoru* V *po řadě na* W_1 *a* W_2. *Pak platí:*

(1) $\boldsymbol{x} \in W_1 \;\Leftrightarrow\; P_{W_1}\boldsymbol{x} = \boldsymbol{x}$.
(2) $\boldsymbol{x} \in W_1^{\perp} \;\Leftrightarrow\; P_{W_1}\boldsymbol{x} = \boldsymbol{0}$.
(3) $W_2 \subseteq W_1 \;\Leftrightarrow\; P_{W_2}(P_{W_1}\boldsymbol{x}) = P_{W_2}\boldsymbol{x}$ *pro každé* $\boldsymbol{x} \in V$.

DŮKAZ. D.46 □

<u>VĚTA</u> 3.77 (Věta o ortogonální projekci)**.**
Nechť $(V, \mathcal{L}_{\mathbb{F}})$ *je VS-prostor,* $V = W \oplus W^{\perp}$ *a* $\widehat{\boldsymbol{x}} = P_W \boldsymbol{x}$ *pro nějaký vektor* $\boldsymbol{x} \in V$. *Pak* $\|\boldsymbol{x} - \widehat{\boldsymbol{x}}\| = \inf_{\boldsymbol{y} \in W} \|\boldsymbol{x} - \boldsymbol{y}\|$ *a* $\widehat{\boldsymbol{x}}$ *je jediný prvek ve* W *s takovou vlastností.*
Je-li $W = \mathcal{L}(E)$, *pak* $\widehat{\boldsymbol{x}} = \beta_1 \boldsymbol{e}_1 + \cdots + \beta_n \boldsymbol{e}_n$ *pro vhodné*[11] *vektory* $\boldsymbol{e}_i \in E$ *a* $\beta_i \in \mathbb{F}$, $i = 1, \ldots, n$, $n \in \mathbb{N}$. *Vektor* $\widehat{\boldsymbol{x}}$ *proto také nazýváme* **nejlepší lineární aproximací** $\boldsymbol{x}$ **pomocí vektorů z** E **podle normy** $\|\cdot\|$. *Je-li* E *ONB ve* W, *pak* $\beta_i = \langle \widehat{\boldsymbol{x}}, \boldsymbol{e}_i \rangle = \langle \boldsymbol{x}, \boldsymbol{e}_i \rangle$ *pro* $i = 1, \ldots, n$.

DŮKAZ. D.47 □

[11] zatímco $\widehat{\boldsymbol{x}}$ je určen jednoznačně, jeho lineární reprezentace pomocí β_j a $\boldsymbol{e}_j \in E$ je jediná jen v případě, že E je báze.

<u>VĚTA</u> 3.78 (Gram-Schmidtova ortogonalizace, `[KaSk:V11.11 s.107]`).
Nechť V je vektorový prostor se skalárním součinem $\langle \cdot, \cdot \rangle$ a nechť $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ ($n \in \mathbb{N}$) je báze[12] *vektorového podprostoru W prostoru V. Položme $W_k := \mathcal{L}(\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_k\})$ pro každé $k \in \mathbb{N}$, $1 \leq k \leq n$ a definujme rekurentně vektory $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n \in V$ takto:*

$$\begin{aligned} \boldsymbol{e}_1 &= \boldsymbol{v}_1, \\ \boldsymbol{e}_k &= \boldsymbol{v}_k - P_{W_{k-1}} \boldsymbol{v}_k = \boldsymbol{v}_k - \sum_{j=1}^{k-1} \frac{\langle \boldsymbol{v}_k, \boldsymbol{e}_j \rangle}{\|\boldsymbol{e}_j\|^2} \boldsymbol{e}_j \quad \text{pro každé } k = 2, \dots, n. \end{aligned}$$

Pak $\mathcal{L}(\{\boldsymbol{e}_1, \dots, \boldsymbol{e}_k\}) = W_k$ pro každé $k = 1, \dots, n$, přičemž vektory $\boldsymbol{e}_1, \dots, \boldsymbol{e}_k$ tvoří ortogonální bázi ve W_k. Zejména tedy vektory $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ tvoří ortogonální bázi ve $W = W_n$.

Důkaz. D.48 $\square$

<u>DŮSLEDEK</u> 3.79 (Důkaz D.49). `[KaSk:V11.12 s.107]`
Každý VS-prostor V konečné dimenze má ortogonální i ortonormální bázi. Přitom každou jeho ortogonální množinu bez nulových prvků lze doplnit na OB ve V a každou jeho ortonormální množinu lze doplnit na ONB ve V.

<u>VĚTA</u> 3.80 (Důkaz D.50).
Pro každý konečně rozměrný podprostor W vektorového prostoru $(V, \mathcal{L}_{\mathbb{F}})$ platí $V = W \oplus W^{\perp}$ a tedy v takovém případě lze vždy použít větu o ortogonální projekci.

Důsledek 3.81.
Nechť $\emptyset \neq M \subseteq V$ je podmnožina VS-prostoru V generující ve V podprostor $\mathcal{L}(M)$ konečné dimenze. Pak $M^{\perp\perp} = \mathcal{L}(M)$.

Důkaz. $W := \mathcal{L}(M), \dim W < \infty \overset{3.80}{\Rightarrow} V = W \oplus W^{\perp} \overset{3.75}{\Rightarrow} W = W^{\perp\perp} = \mathcal{L}(M)^{\perp\perp} \overset{3.71}{=} M^{\perp\perp}$. $\square$

[12] algoritmus lze po modifikaci užít i v případě, že $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ pouze generují prostor V: v rekurzi pro $\boldsymbol{e}_k$ sčítáme jen přes ta j, pro něž $\boldsymbol{e}_j \neq \boldsymbol{0}$; bázi pak tvoří jen nenulové vektory $\boldsymbol{e}_j$.

VĚTA 3.82 (Důkaz D.51).
Nechť $(V_1, \mathcal{L}_{\mathbb{F}})$ *a* $(V_2, \mathcal{L}_{\mathbb{F}})$ *jsou dva VS-prostory a* $T : V_1 \to V_2$ *lineární operátor. Jestliže existuje zobrazení* $T^* : V_2 \to V_1$ *takové, že* $\langle T\boldsymbol{x}, \boldsymbol{y}\rangle = \langle \boldsymbol{x}, T^*\boldsymbol{y}\rangle$ *platí pro každé* $\boldsymbol{x} \in V_1$ *a* $\boldsymbol{y} \in V_2$, *pak* T^* *je jediné takové a určuje lineární operátor nazývaný* **operátorem adjungovaným k** T. *Je-li* $V_1 = V_2$ *a* $T = T^*$, *pak* T *se nazývá* **samoadjungovaný operátor**.

Věta 3.83.
Je-li T *lineární operátor jako v 3.82 a* $\dim \mathcal{R}(T) =: n < \infty$ *pak* T^* *existuje a zkonstruuje se takto:*

(1) *V* $\mathcal{R}(T)$ *vybereme nějakou* n*-prvkovou ortonormální bázi* E' *a* $\boldsymbol{b}_1, \dots, \boldsymbol{b}_n \in V_1$ *takové, že* $E' = \{T(\boldsymbol{b}_1), \dots, T(\boldsymbol{b}_n)\}$.
(2) *Pak* $B := \{\boldsymbol{b}_1, \dots, \boldsymbol{b}_n\}$ *je lineárně nezávislá ve* V_1 *a tedy generuje ve* V_1 *podprostor* $W := \mathcal{L}(B)$ *rovněž dimenze* n.
(3) *Nechť* $E =: \{\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\}$ *je ONB ve* W *získaná Gram-Schmidtovou ortogonalizací báze* B *dle 3.78.*
(4) *Pro každé* $\boldsymbol{y} \in V_2$ *položíme* $T^*\boldsymbol{y} := \sum_{j=1}^{n} \langle \boldsymbol{y}, T\boldsymbol{e}_j\rangle \boldsymbol{e}_j$.

POZNÁMKA 3.84. Každý lineární operátor $V_1 \to V_2$ určuje vztahem $\langle T\boldsymbol{x}, \boldsymbol{y}\rangle$ bilineární formu $V_1 \times V_2 \to \mathbb{F}$ (srov. 3.60), kterou lze vzhledem k linearitě T opět upravovat podle vztahů analogických k (3.1):

$$\langle T(\sum_{i=1}^{n} \xi_i \boldsymbol{x}_i), \sum_{j=1}^{m} \eta_j \boldsymbol{y}_j\rangle = \sum_{i=1}^{n}\sum_{j=1}^{m} \xi_i \overline{\eta}_j \langle T\boldsymbol{x}_i, \boldsymbol{y}_j\rangle. \tag{3.3}$$

Je-li $V := V_1 = V_2$, pak zobrazení $V \to V$ definované vztahem $\langle T\boldsymbol{x}, \boldsymbol{x}\rangle$ nazýváme **kvadratickou formou**. Pokud navíc platí $T = T^*$, pak tato forma nabývá pouze reálných hodnot, neboť
$\langle T\boldsymbol{x}, \boldsymbol{x}\rangle = \langle \boldsymbol{x}, T\boldsymbol{x}\rangle \overset{(S3)}{=} \overline{\langle T\boldsymbol{x}, \boldsymbol{x}\rangle}$.
Samoadjungovaný operátor T se nazývá **(striktně) pozitivní**, jestliže $\langle T\boldsymbol{x}, \boldsymbol{x}\rangle \geq 0$ pro každé $\boldsymbol{x} \in V$ ($\langle T\boldsymbol{x}, \boldsymbol{x}\rangle > 0$ pro každé $\boldsymbol{x} \neq \boldsymbol{0}$), neboli když jím určená kvadratická forma nabývá pouze nezáporných hodnot (kladných hodnot pro nenulová $\boldsymbol{x}$). Píšeme $T \geq 0$ ($T > 0$).

VĚTA 3.85 (Vlastnosti adjungovaných operátorů, Důkaz D.52).
Nechť $(V_1, \mathcal{L}_{\mathbb{F}})$, $(V_2, \mathcal{L}_{\mathbb{F}})$ *a* $(V_3, \mathcal{L}_{\mathbb{F}})$ *jsou VS-prostory,* $T : V_1 \to V_2$ *a* $U : V_2 \to V_3$ *lineární operátory a* $T^* : V_2 \to V_1$ *a* $U^* : V_3 \to V_2$ *operátory k nim adjungované. Pak platí*

(1) T *je operátor adjungovaný k* T^**, tj. platí* $T^{**} = T$.
(2) T^*U^* *je operátor adjungovaný ke složenému operátoru* $UT : V_1 \to V_3$*, tj. platí* $(UT)^* = T^*U^*$.
(3) *Identický operátor* $I : V_1 \to V_1$ *je samoadjungovaný, tj.* $I^* = I$.
(4) TT^* *i* T^*T *jsou pozitivní operátory a tedy také samoadjungované.*

Věta 3.86 (Charakterizace ortogonální projekce, Důkaz D.53).
Nechť $(V, \mathcal{L}_{\mathbb{F}})$ *je VS-prostor a* P *surjektivní zobrazení* V *na nějaký jeho podprostor* W*. Pak následující výroky jsou ekvivalentní:*

(1) $P = P_W$*, tj.* P *je operátor ortogonální projekce* V *na* W.
(2) *Pro každé* $\boldsymbol{x} \in V$ *platí* $\boldsymbol{x} - P\boldsymbol{x} \perp W$.
(3) P *je lineární operátor s vlastnostmi:* $P^2 = P$ *(tj.* P *je projekční) a* $P = P^*$ *(tj.* P *je samoadjungovaný).*

Důsledek 3.87 (Důkaz D.54).
Každý operátor ortogonální projekce je pozitivní.

Věta 3.88 (ilustrační obr. `V3-88obr.tif(->ZIP)`, **Důkaz D.55**).
Nechť $(V_1, \mathcal{L}_{\mathbb{F}})$, $(V_2, \mathcal{L}_{\mathbb{F}})$ *jsou VS-prostory,* $T : V_1 \to V_2$ *lineární operátor a* $T^* : V_2 \to V_1$ *operátor k němu adjungovaný. Pak platí:*

(1) $\mathcal{N}(T) = \mathcal{R}(T^*)^\perp$ *a* $\mathcal{N}(T^*) = \mathcal{R}(T)^\perp$.
(2) $T = T^* \Rightarrow \mathcal{N}(T) = \mathcal{R}(T)^\perp$.
(3) $\mathcal{N}(T^*T) = \mathcal{N}(T)$ *a* $\mathcal{N}(TT^*) = \mathcal{N}(T^*)$.
(4) T *surjektivní* $\Rightarrow T^*$ *je izomorfní vnoření.*
T^* *surjektivní* $\Rightarrow T$ *je izomorfní vnoření.*
(5) *Jestliže* $\dim \mathcal{R}(T) < \infty$ *nebo* $\dim \mathcal{R}(T^*) < \infty$*, pak*
 (i) $V_1 = \mathcal{R}(T^*) \oplus \mathcal{N}(T), V_2 = \mathcal{R}(T) \oplus \mathcal{N}(T^*)$,
 (ii) $\mathcal{N}(T)^\perp = \mathcal{R}(T^*), \mathcal{N}(T^*)^\perp = \mathcal{R}(T)$,

(iii) $\mathcal{R}(T^*T) = \mathcal{R}(T^*)$ *a* $\mathcal{R}(TT^*) = \mathcal{R}(T)$.
(iv) $T^*|_{\mathcal{R}(T)} : \mathcal{R}(T) \to \mathcal{R}(T^*)$ *i* $T|_{\mathcal{R}(T^*)} : \mathcal{R}(T^*) \to \mathcal{R}(T)$ *jsou izomorfizmy a tedy* $\dim \mathcal{R}(T) = \dim \mathcal{R}(T^*) =: n$.
(v) $\dim V_1 = n + \dim \mathcal{N}(T)$ *a* $\dim V_2 = n + \dim \mathcal{N}(T^*)$.
(vi) *T izomorfizmus $\Rightarrow$ T^* je izomorfizmus, $(T^{-1})^*$ existuje a platí $(T^{-1})^* = (T^*)^{-1}$.*

DEFINICE 3.89. Lineární operátor z VS-prostoru V_1 do VS-prostoru V_2 se nazývá **unitární (ortogonální**[13]**)**, jestliže zobrazuje nějakou ONB ve V_1 na ONB ve V_2 o stejné mohutnosti. Každý unitární operátor je dle 3.30(4) izomorfizmem, nazývá se proto také **unitárním izomorfizmem** prostorů V_1 a V_2.
Jestliže existuje unitární operátor V_1 na V_2, pak říkáme, že prostory V_1 a V_2 jsou **unitárně izomorfní** a píšeme $(V_1, \mathcal{L}_{\mathbb{F}}) \overset{U}{\simeq} (V_2, \mathcal{L}_{\mathbb{F}})$. Jestliže V_1 je unitárně izomorfní pouze s nějakým podprostorem ve V_2, pak píšeme $(V_1, \mathcal{L}_{\mathbb{F}}) \overset{U}{\precsim} (V_2, \mathcal{L}_{\mathbb{F}})$ a každý unitární operátor V_1 na $\mathcal{R}(V_1) \subseteq V_2$ nazýváme **unitárně izomorfním vnořením V_1 do V_2**.

VĚTA 3.90 (Charakterizace unitárních operátorů, Důkaz D.56)**.**
Nechť $(V_1, \mathcal{L}_{\mathbb{F}})$, $(V_2, \mathcal{L}_{\mathbb{F}})$ jsou VS-prostory a existuje ONB ve V_1. Nechť dále $T : V_1 \to V_2$ je lineární operátor. Pak následující výroky jsou ekvivalentní:
(1) *T je unitární.*
(2) *T zobrazuje každou ONB ve V_1 na ONB ve V_2 o stejné mohutnosti.*
(3) *T je surjekce zachovávající skalární součin:* $\langle T\boldsymbol{x}, T\boldsymbol{y}\rangle = \langle \boldsymbol{x}, \boldsymbol{y}\rangle$ *pro každé* $\boldsymbol{x}, \boldsymbol{y} \in V_1$.
(4) *T je surjekce zachovávající normu (tzv.* **izometrie***):* $\|T\boldsymbol{x}\| = \|\boldsymbol{x}\|$ *pro každé* $\boldsymbol{x} \in V_1$.
(5) *T^* existuje a platí $T^* = T^{-1}$.*
(6) *T^* existuje a T^*T je identický operátor.*

[13]Termín *ortogonální* se obvykle užívá v případě reálných prostorů ($\mathbb{F} = \mathbb{R}$).

V takovém případě $T^{-1} = T^*$ je rovněž unitární operátor z V_2 na V_1 a platí nejen $T^*T = I_{V_1}$ dle (6), ale i $TT^* = I_{V_2}$.

DŮSLEDEK 3.91 (Charakterizace unitárně izomorfních vnoření)**.**
Za předpokladů předchozí věty jsou ekvivalentní následující výroky:

(1') *T je unitárně izomorfní vnoření.*
(2') *T zobrazuje každou ONB ve V_1 na ortonormální množinu ve V_2 o stejné mohutnosti.*
(3') *T zachovává skalární součin:*
$\langle T\boldsymbol{x}, T\boldsymbol{y}\rangle = \langle \boldsymbol{x}, \boldsymbol{y}\rangle$ *pro každé* $\boldsymbol{x}, \boldsymbol{y} \in V_1$.
(4') *T zachovává normu: $\|T\boldsymbol{x}\| = \|\boldsymbol{x}\|$ pro každé $\boldsymbol{x} \in V_1$.*
(5') *$T^* : \mathcal{R}(T) \to V_1$ existuje a platí $T^* = T^{-1}$ na $\mathcal{R}(T)$.*
(6') *T^* existuje a T^*T je identický operátor.*

V takovém případě $T^{-1} = T^*$ je rovněž unitární operátor z $\mathcal{R}(T)$ na V_1 a platí nejen $T^*T = I_{V_1}$ dle (6'), ale i $TT^* = I_{\mathcal{R}(T)}$.

Důkaz. Je přímým důsledkem věty 3.90, jestliže uvážíme, že $T : V_1 \to V_2$ je unitárně izomorfním vnořením právě když $T : V_1 \to \mathcal{R}(T)$ je unitárním izomorfizmem. Stačí tedy ve formulacích dle potřeby V_2 zaměnit za $\mathcal{R}(T)$. Přitom surjektivita na $\mathcal{R}(T)$ je automatická, takže tento požadavek lze ve (3') a (4') vypustit. □

DŮSLEDEK 3.92 (Důkaz D.57)**.**
Je-li $(V, \mathcal{L}_{\mathbb{F}})$ VS-prostor konečné dimenze n, a E jeho ONB, pak izomorfizmus $[\cdot]_E : V \to \mathbb{F}^n$ z věty 3.32 je dokonce unitární izomorfizmus $(V, \mathcal{L}_{\mathbb{F}})$ na $(\mathbb{F}^n, \mathcal{L}_{\mathbb{F}})$.

DŮSLEDEK 3.93 (Důkaz D.58)**.**

(1) *Dva konečně rozměrné reálné (komplexní) VS-prostory V_1 a V_2 mají stejnou dimenzi právě když $(V_1, \mathcal{L}_{\mathbb{F}}) \overset{U}{\simeq} (V_2, \mathcal{L}_{\mathbb{F}})$.*
(2) *Pro dva konečně rozměrné reálné (komplexní) VS-prostory $(V_1, \mathcal{L}_{\mathbb{F}})$, $(V_2, \mathcal{L}_{\mathbb{F}})$ platí $\dim V_1 \le \dim V_2$ právě když $(V_1, \mathcal{L}_{\mathbb{F}}) \overset{U}{\precsim} (V_2, \mathcal{L}_{\mathbb{F}})$.*

ANGLICKÁ TERMINOLOGIE Z LINEÁRNÍ ALGEBRY

skalár ♦ scalar
skalární součin ♦ dot product
vektor ♦ vector
vektorový (lineární) prostor ♦ vector (linear) space
podprostor ♦ subspace
lineární kombinace ♦ linear combination
lineární obal ♦ linear span
(lineárně) generovaný (čím) ♦ spanned by
báze ♦ basis
lineárně (ne)závislý ♦ linearly (in)dependent
dimenze ♦ dimension
n-dimenzionální ♦ n-dimensional
vícerozměrný ♦ multivariate
lineární zobrazení (operátor) ♦ linear mapping (operator)
vnoření ♦ embedding
nulový podprostor (jádro) operátoru ♦ null space
prostor hodnot operátoru ♦ range space
souřadnice ♦ co-ordinates
faktor prostor ♦ factor space
kongruentní modulo ♦ congruent modulo
(přímý) součet ♦ (direct) sum
přímý doplněk ♦ direct complement
projekční operátor ♦ projection operator
norma ♦ norm
normovaný prostor ♦ normed space
vnitřní (skalární) součin ♦ inner (scalar) product
prostor s vnitřním součinem ♦ inner product space
bilineární forma ♦ bilinear form
kvadratická forma ♦ quadratic form
Pythagorova věta ♦ Pythagorean theorem
rovnoběžníkový zákon ♦ parallelogram law
úhel mezi ♦ angle between

kolmý, ortogonální ⧫ perpendicular, orthogonal
ortonormální ⧫ orthonormal
ortogonální doplněk ⧫ orthogonal complement
ortogonální součet ⧫ orthogonal sum
ortogonální projekce ⧫ orthogonal projection
nejlepší lineární aproximace ⧫ best linear approximation
ortogonalizace ⧫ orthogonalization
(samo)adjungovaný ⧫ (self-)adjoint
(striktně) pozitivní ⧫ (strictly) positive
unitární operátor ⧫ unitary operator
unitárně izomorfní ⧫ unitary isomorphic

4. Teorie matic

Teorie a příklady: `[KaSk: s.63-129]`, `[Šik: s.1-23]`
Příklady: `[Ho:řešené č.16-36; s.17-37]`,
`[Ho:neřešené kap.4, 5 s.100-137]`

Teorie matic představuje formální kalkulus pro manipulaci s vektory a lineárními zobrazeními ve VS-prostoru $(\mathbb{F}^n, \mathcal{L}_{\mathbb{F}})$. Prostřednictvím unitárního izomorfizmu z 3.92 lze tento aparát užít i pro jakýkoli abstraktní vektorový prostor $(V, \mathcal{L}_{\mathbb{F}})$ konečné dimenze.

Numerické výpočetní prostředí MATLAB používá matice nad komplexními čísly ($\mathbb{F} = \mathbb{C}$) jako základní proměnné a je tedy ideálním výpočetním prostředím pro řešení úloh lineárního charakteru. Má však daleko širší záběr i nad tento lineární rámec.

Název systému je odvozen z angličtiny: MATLAB=MATrix LABoratory. Systém produkuje americká společnost *MathWorks, Inc.* (`http://www.mathworks.com`) a jejím výhradním distributorem pro Českou republiku je pražská firma *Humusoft, s.r.o.* (`http://www.humusoft.cz`). Obecně lze systém MATLAB charakterizovat jako maticově orientované výpočetní prostředí s vlastním programovacím jazykem vhodným pro efektivní implementaci, provádění a vizualizaci numerických výpočtů vyžadujících náročný aparát z nejrůznějších oblastí matematiky. Je dostupný na všech běžných platformách (WINDOWS, LINUX, UNIX, atd.) při zachování takřka stoprocentní přenositelnosti vytvořených programů a datových souborů.

Vzhledem ke svému snadnému a intuitivnímu ovládání bude proto MATLAB nadále využíván k demonstracím i ve cvičeních.

Cvičení v MATLABu: `tmcv1`, `tmcv2`, `tmcv3`, `tmcv4`

4.1. MATICE A JEJICH ZÁKLADNÍ DRUHY.

DEFINICE 4.1. Nechť I a J jsou konečné lineárně uspořádané množiny ($m := \operatorname{card} I$, $n := \operatorname{card} J$), pak každé zobrazení $A : I \times J \to \mathbb{F}$ nazýváme **maticí nad $\mathbb{F}$ typu m/n (rozměru $m \times n$)**. Pro každé $i \in I$ a $j \in J$ značíme hodnotu tohoto zobrazení jako $a_{ij} := A(i,j)$ ($a_{ij} \in \mathbb{F}$) a nazýváme **prvkem matice $\boldsymbol{A}$ v i-tém řádku a j-tém sloupci** nebo také **(i,j)-tým prvkem matice $\boldsymbol{A}$**.
Množina I, resp. J se nazývá **množinou řádkových, resp. sloupcových indexů matice $\boldsymbol{A}$**. V dalším se bez újmy na obecnosti můžeme omezit na standardně užívané indexové množiny $I = \{1, 2, \ldots, m\}$ a $J = \{1, 2, \ldots, n\}$. Matici $\boldsymbol{A}$ pak zapisujeme jako podrobný výčet všech jejích prvků uspořádaný do tabulky:

$$\boldsymbol{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}. \tag{4.1}$$

Pokud a_{ij} nepředstavují konkrétní hodnoty, vystačíme se zjednodušeným symbolickým zápisem $\boldsymbol{A} = [a_{ij}]$. Speciální případy:

- $m = n$: $\boldsymbol{A}$ nazýváme **čtvercovou maticí řádu m**.
- $m = 1$: $\boldsymbol{A}$ nazýváme **řádkovým vektorem délky n**.
- $n = 1$: $\boldsymbol{A}$ nazýváme **sloupcovým vektorem délky m**.
- $m = n = 1$: $\boldsymbol{A}$ ztotožňujeme s jejím jediným prvkem, tj. $[a] = a$.
- $m = 0$: $\boldsymbol{A}$ nazýváme **prázdným řád. vektorem délky n**.
- $n = 0$: $\boldsymbol{A}$ nazýváme **prázdným sloup. vektorem délky m**.
- $m = n = 0$: $\boldsymbol{A}$ nazýváme **prázdnou maticí typu $0/0$**.

Je-li $m = 0$ nebo $n = 0$, pak $\boldsymbol{A}$ se nazývá **prázdná matice**[14]. Píšeme $\boldsymbol{A} = [\ ]$.

---

[14]Prázdná matice koresponduje s prázdným zobrazením zavedeným v poznámce 1.36(4).

DEFINICE 4.2 (Submatice)**.**
Matici $B =: [b_{kl}]$ nazveme **submaticí** matice $\boldsymbol{A} =: [a_{ij}]$, jestliže existují řádkové indexy $1 \leq i_1 < i_2 < \cdots < i_p \leq m$ a sloupcové indexy $1 \leq j_1 < j_2 < \cdots < j_q \leq n$ tak, že $b_{kl} = a_{i_k j_l}$ pro každé $k = 1, \dots, p$ a $l = 1, \dots, q$. Píšeme $B = A([i_1, \dots, i_p], [j_1, \dots, j_q])$.
Speciální případy:

- $p = m$ (vybrány všechny řádky): $B =: A(:, [j_1, \dots, j_q])$,
- $q = n$ (vybrány všechny sloupce): $B =: A([i_1, \dots, i_p], :)$,
- $p = 1$ (vybrán jeden řádek $i := i_1$): $B =: A(i, [j_1, \dots, j_q])$,
- $q = 1$ (vybrán jeden sloupec $j := j_1$): $B =: A([i_1, \dots, i_p], j)$,
- i-tý řádek matice $\boldsymbol{A}$: $B =: A(i, :)$,
- j-tý sloupec matice $\boldsymbol{A}$: $B =: A(:, j)$.

Poznámka 4.3.

(1) Matice lze sestavovat i po blocích ve tvaru (4.1), kde a_{ij} mohou být nahrazeny submaticemi A_{ij} kompatibilních rozměrů. Při sestavování matice pomocí bloků skládaných vedle sebe (pod sebe) budeme v souladu se syntaxí jazyka MATLAB v zápisech užívat jako oddělovače čárku (středník). Například matici $\boldsymbol{A}$ ze (4.1) můžeme pomocí jejích sloupců $\boldsymbol{s}_j := A(:, j)$, resp. řádků $\boldsymbol{r}_i := A(i, :)$ zapsat také takto:
$\boldsymbol{A} = [\boldsymbol{s}_1, \dots, \boldsymbol{s}_n]$, resp. $\boldsymbol{A} = [\boldsymbol{r}_1; \dots; \boldsymbol{r}_m]$.

(2) Ztotožníme-li řádkové, resp. sloupcové vektory délky n s prvky vektorového prostoru $\mathbb{F}^n$, můžeme matici $\boldsymbol{A}$ typu m/n interpretovat dvojím způsobem:
a) jako uspořádaný systém m řádkových vektorů z $\mathbb{F}^n$,
b) jako uspořádaný systém n sloupcových vektorů z $\mathbb{F}^m$.
Takový systém může v příslušném prostoru hrát roli systému generátorů nějakého podprostoru, jeho báze apod.

Označení .
$\mathcal{M}_{m,n} := \mathcal{M}_{m,n}(\mathbb{F}) \dots$ množina všech matic nad $\mathbb{F}$ typu m/n,

$\delta_{ij} = \begin{cases} 1 \text{ pro } i = j \\ 0 \text{ pro } i \neq j \end{cases}$ ... **Kroneckerův symbol** δ.

$\boldsymbol{x} \in \mathbb{F}^n$ ... sloupcový vektor (pokud nebude řečeno jinak).
$\boldsymbol{\varepsilon}_i := [\delta_{1,i}; \delta_{2,i}; \dots; \delta_{n,i}]$ ... i-tý prvek přirozené báze $\mathcal{E}$ dle 3.25(4).
$\boldsymbol{I}_n := [\delta_{i,j}]$ ... **jednotková matice** řádu n: $I_n(i,:) = I_n(:,i) = \boldsymbol{\varepsilon}_i$;
její i-tý řádek (sloupec) je právě $\boldsymbol{\varepsilon}_i$, pokud neděláme rozdíl mezi řádkovou či sloupcovou formou zápisu.
$\mathbf{0}_{m,n}$ ... **nulová matice** typu m/n: všechny prvky jsou nuly.
$\mathbf{1}_{m,n}$ ... **matice jedniček** typu m/n: všechny prvky jsou jedničky.
$\boldsymbol{E}_{ij} \in \mathcal{M}_{m,n}$ ... matice, kde $E_{ij}(i,j) = 1$ a ostatní prvky jsou nuly.
$\operatorname{diag}(\boldsymbol{A}) =: [a_{11}, a_{22}, \dots]$ ... **hlavní diagonála matice** A.
$[a_{1n}, a_{2,n-1}, a_{3,n-2}, \dots]$ ... **vedlejší diagonála matice** A.

Poznámka 4.4. Je-li $\boldsymbol{x} = [x_1; \dots; x_n]$, pak zřejmě $\boldsymbol{x} = \sum_{i=1}^{n} x_i \boldsymbol{\varepsilon}_i$ a tedy složky x_i jsou dle 3.31 přímo souřadnicemi $\boldsymbol{x}$ v přirozené bázi. Tudíž $\boldsymbol{x} = [\boldsymbol{x}]_{\mathcal{E}}$ a zobrazení $[\cdot]_{\mathcal{E}} : \mathbb{F}^n \to \mathbb{F}^n$ je identita.

DEFINICE 4.5 (Matice se speciální strukturou).
Konstantní matice: $\boldsymbol{A} = [a_{ij}]$, kde $a_{ij} = a \ \forall\, i,j$, neboli matice, jejíž všechny prvky jsou stejné, například $\mathbf{0}_{m,n}$ a $\mathbf{1}_{m,n}$.
Diagonální matice: $\boldsymbol{D} = [d_{ij}]$, $d_{ij} = 0$ pro $\forall\, i \neq j$,
neboli matice, která má všechny prvky mimo hlavní diagonálu nulové.
$\operatorname{diag}(\boldsymbol{d})$, $\operatorname{diag}(d_1, \dots, d_n)$ ... čtvercová diagonální matice řádu n s hlavní diagonálou $\boldsymbol{d} = [d_1, \dots, d_n]$.
Symetrická matice: $\boldsymbol{A} = [a_{ij}]$, $a_{ij} = a_{ji} \ \forall\, i,j$,
neboli matice se stejnými řádky a sloupci: $A(i,:) = A(:,i) \ \forall\, i$ (symetrie vzhledem k hlavní diagonále).
Antisymetrická matice: $\boldsymbol{A} = [a_{ij}]$, $a_{ij} = -a_{ji} \ \forall\, i,j$, neboli matice, kde řádky a sloupce mají opačné znaménko: $A(i,:) = -A(:,i) \ \forall\, i$ (antisymetrie vzhledem k hlavní diagonále). Jelikož $a_{ii} = -a_{ii}$, tak každá antisymetrická matice má nulovou hlavní diagonálu.
Hermitovsky symetrická matice ($\mathbb{F} \subseteq \mathbb{C}$): $\boldsymbol{A} = [a_{ij}]$, $a_{ij} = \overline{a}_{ji} \ \forall\, i,j$, neboli matice, kde řádky a sloupce jsou vůči sobě komplexně sdružené: $A(i,:) = \overline{A(:,i)} \ \forall\, i$ (hermitovská symetrie vzhledem k hlavní diagonále). Jelikož $a_{ii} = \overline{a}_{ii}$, tak každá hermitovsky symetrická matice má na hlavní diagonále reálná čísla.

Je-li $a_{ij} \in \mathbb{R}\ \forall\, i, j$, pak hermitovská symetrie je zřejmě ekvivalentní se symetrií.

Hermitovsky antisymetrická matice ($\mathbb{F} \subseteq \mathbb{C}$): $\boldsymbol{A} = [a_{ij}]$, $a_{ij} = -\overline{a}_{ji}$ $\forall\, i, j$ (tj. $\mathrm{Re}\, a_{ij} = -\mathrm{Re}\, a_{ji}$ a $\mathrm{Im}\, a_{ij} = \mathrm{Im}\, a_{ji}$),
neboli matice, kde řádky a sloupce se liší znaménkem v reálné části: $A(i,:) = -\overline{A(:,i)}\ \forall\, i$ (hermitovská antisymetrie vzhledem k hlavní diagonále). Jelikož $a_{ii} = -\overline{a}_{ii}$, tak každá hermitovsky antisymetrická matice má na hlavní diagonále ryze imaginární čísla nebo nuly.

Je-li $a_{ij} \in \mathbb{R}\ \forall\, i, j$, pak hermitovská antisymetrie je zřejmě ekvivalentní s antisymetrií.

Horní trojúhelníková matice: $\boldsymbol{U} = [u_{ij}]$, $u_{ij} = 0$ pro $\forall\, i > j$,
neboli matice, která má všechny prvky pod hlavní diagonálou nulové.

Dolní trojúhelníková matice: $\boldsymbol{L} = [l_{ij}]$, $l_{ij} = 0$ pro $\forall\, i < j$,
neboli matice, která má všechny prvky nad hlavní diagonálou nulové.

Schodovitá matice: $\boldsymbol{S} = [s_{ij}]$ matice $m \times n$, která je buď nulová nebo existují přirozená čísla $k \leq m$ a $1 \leq j_1 < j_2 < \ldots < j_k \leq n$ s těmito vlastnostmi:

(a) $s_{ij_i} \neq 0$ pro $1 \leq i \leq k$,
(b) $s_{ir} = 0$ pro $1 \leq i \leq k,\ 1 \leq r < j_i$,
(c) $s_{ij} = 0$ pro $k < i \leq m,\ 1 \leq j \leq n$.

Snadno jako cvičení se dokáže následující věta.

VĚTA 4.6. *Nechť* $\boldsymbol{S}$ *je nenulová schodovitá matice jako v definici 4.5, pak* $S([1,\ldots,k],[j_1,\ldots,j_k])$ *je její horní trojúhelníková submatice s nenulovými prvky* s_{ij_i} *na hlavní diagonále.*

4.2. **ZÁKLADNÍ MATICOVÉ OPERACE.**

V hranaté závorce za názvem operace uvádíme její syntaxi v MATLABu.

DEFINICE 4.7 (LINEÁRNÍ OPERACE).
Operace sečítání matic téhož typu, výběru opačné matice a násobení matice skalárem definujeme po složkách:
Sečítání [`X = A + B`]:

$$\underset{m\times n}{\boldsymbol{X}} = \underset{m\times n}{\boldsymbol{A}} + \underset{m\times n}{\boldsymbol{B}} \overset{\text{def.}}{\equiv} X(i,j) := A(i,j) + B(i,j)\ \forall i,j.$$

Opačná matice [`X = -A`]:

$$\underset{m\times n}{\boldsymbol{X}} = -\underset{m\times n}{\boldsymbol{A}} \overset{\text{def.}}{\equiv} X(i,j) := -A(i,j)\ \forall i,j.$$

Násobení matice skalárem $a \in \mathbb{F}$ [`X = a*A`]:

$$\underset{m\times n}{\boldsymbol{X}} = a\underset{m\times n}{\boldsymbol{A}} \overset{\text{def.}}{\equiv} X(i,j) := aA(i,j)\ \forall i,j.$$

DEFINICE 4.8 (TRANSFORMACE MATICE NA VEKTOR).
Operátor $\mathrm{vec} : \mathcal{M}_{mn} \to \mathbb{F}^{mn}$ [`A(:)`]:
$\mathrm{vec}\underset{m\times n}{\boldsymbol{A}} := [A(:,1); A(:,2); \ldots ; A(:,n)]$.
Tento operátor skládá tedy sloupce matice $\boldsymbol{A}$ pod sebe do sloupcového vektoru.

Věta 4.9. *Stejně jako v příkladu 3.4(4) tvoří množina všech matic $\mathcal{M}_{m,n}$ opatřená výše uvedenými operacemi vektorový prostor $(\mathcal{M}_{m,n}, \mathcal{L}_{\mathbb{F}})$ s nulovou maticí $\mathbf{0}_{m,n}$ jako nulovým prvkem. Operátor* vec *je zřejmě lineární a dokonce izomorfizmus vektorových prostorů $(\mathcal{M}_{m,n}, \mathcal{L}_{\mathbb{F}})$ a $(\mathbb{F}^{mn}, \mathcal{L}_{\mathbb{F}})$. Uvážíme-li 3.33 a 3.25(4), pak $\dim \mathcal{M}_{m,n} = mn$, přičemž roli přirozené báze v $\mathcal{M}_{m,n}$ hraje systém matic $\boldsymbol{E}_{ij}$ ($i = 1,\ldots,m$; $j = 1\ldots,n$).*

DEFINICE 4.10 (TRANSPOZICE MATIC).
Transponovaná matice [`X = A.'`]:

$$\underset{n\times m}{\boldsymbol{X}} = \underset{m\times n}{\boldsymbol{A}^T} \overset{\text{def.}}{\equiv} X(i,j) := A(j,i)\ \forall i,j.$$

Tento operátor zaměňuje sloupce a řádky, tj.:
$X(i,:) = A(:,i)$ nebo ekvivalentně $X(:,i) = A(i,:)\ \forall\, i$.

Hermitovsky (konjugovaně) transponovaná matice ($\mathbb{F} \subseteq \mathbb{C}$) [`X = A'`]:

$\underset{n\times m}{\boldsymbol{X}} = \underset{m\times n}{\boldsymbol{A}^*} \overset{\text{def.}}{\equiv} X(i,j) := \overline{A}(j,i)\ \forall i,j.$

Tento operátor zaměňuje řádky (resp. sloupce) za komplexně sdružené sloupce (resp. řádky):
$X(i,:) = \overline{A}(:,i)$, resp. ekvivalentně $X(:,i) = \overline{A}(i,:)\ \forall\, i$.

Transpoziční operátory mají zřejmě následující vlastnosti:

<u>VĚTA</u> 4.11 (Vlastnosti (hermitovské) transpozice)**.**

(1) $(\boldsymbol{A}+\boldsymbol{B})^T = \boldsymbol{A}^T + \boldsymbol{B}^T$, $(\boldsymbol{A}+\boldsymbol{B})^* = \boldsymbol{A}^* + \boldsymbol{B}^*$.
(2) $(a\boldsymbol{A})^T = a\boldsymbol{A}^T$, $(a\boldsymbol{A})^* = \overline{a}\boldsymbol{A}^*\ \forall\, a \in \mathbb{F}$.
(3) $\boldsymbol{0}^*_{m,n} = \boldsymbol{0}^T_{m,n} = \boldsymbol{0}_{n,m}$, $\boldsymbol{1}^*_{m,n} = \boldsymbol{1}^T_{m,n} = \boldsymbol{1}_{n,m}$,
$\boldsymbol{E}^*_{ij} = \boldsymbol{E}^T_{ij} = \boldsymbol{E}_{ji}\ \forall\, i,j$.
(4) $(\boldsymbol{A}^T)^T = \boldsymbol{A}$, $(\boldsymbol{A}^*)^* = \boldsymbol{A}$.
(5) $\boldsymbol{A}$ *reálná* $\Rightarrow \boldsymbol{A}^* = \boldsymbol{A}^T$.
(6) $\boldsymbol{A}$ *je symetrická* $\Leftrightarrow\ \boldsymbol{A}^T = \boldsymbol{A}$,
$\boldsymbol{A}$ *je hermitovsky symetrická* $\Leftrightarrow\ \boldsymbol{A}^* = \boldsymbol{A}$.
(7) $\boldsymbol{D}$ *diagonální* $\Rightarrow \boldsymbol{D}^T = \boldsymbol{D}$, *zejména platí* $\boldsymbol{I}^*_n = \boldsymbol{I}^T_n = \boldsymbol{I}_n$.
(8) $\boldsymbol{A}$ *horní (dolní) trojúhelníková* $\Rightarrow \boldsymbol{A}^*$ *i* $\boldsymbol{A}^T$ *jsou dolní (horní) trojúhelníkové matice.*
(9) $a(\boldsymbol{A}+\boldsymbol{A}^T)$, *resp.* $a(\boldsymbol{A}-\boldsymbol{A}^T)$ *je symetrická, resp. antisymetrická matice pro každou čtvercovou matici* $\boldsymbol{A}$ *a každé* $a \in \mathbb{F}$.
(10) $a(\boldsymbol{A}+\boldsymbol{A}^*)$, *resp.* $a(\boldsymbol{A}-\boldsymbol{A}^*)$ *je hermitovsky symetrická, resp. hermitovsky antisymetrická matice pro každou čtvercovou matici* $\boldsymbol{A}$ *a každé* $a \in \mathbb{R}$.
(11) *Každou čtvercovou matici* $\boldsymbol{A}$ *lze rozložit na její (hermitovsky) symetrickou a antisymetrickou část:*
$\boldsymbol{A} = \frac{1}{2}(\boldsymbol{A}+\boldsymbol{A}^T) + \frac{1}{2}(\boldsymbol{A}-\boldsymbol{A}^T)$, $\boldsymbol{A} = \frac{1}{2}(\boldsymbol{A}+\boldsymbol{A}^*) + \frac{1}{2}(\boldsymbol{A}-\boldsymbol{A}^*)$.

Poznámka 4.12.
Jelikož transpozice transformuje sloupcový (řádkový) vektor na řádkový (sloupcový), platí zejména $[x_1; \ldots; x_n] = [x_1, \ldots, x_n]^T$.
V dalším budeme pro zápis sloupcových vektorů přednostně užívat tvar $[x_1, \ldots, x_n]^T$, který je v matematice standardní (užívání středníku je totiž motivováno pouze syntaxí jazyka MATLAB).

DEFINICE 4.13 (MULTIPLIKATIVNÍ OPERACE).
Maticové násobení [`X = A * B`]:

$$\underset{m\times p}{\boldsymbol{X}} = \underset{m\times n}{\boldsymbol{A}} \,.\, \underset{n\times p}{\boldsymbol{B}} \quad \overset{\text{def.}}{\equiv} \quad X(i,j) := \textstyle\sum_{k=1}^{n} A(i,k).B(k,j)\ \forall i,j.$$

Výše uvedené lze ekvivalentně vyjádřit dvojím způsobem:

a) $X(:,j) = \sum_{k=1}^{n} A(:,k).B(k,j)\ \forall j \ldots$ j-tý sloupec X je lineární kombinací sloupců matice $\boldsymbol{A}$ pomocí koeficientů z j-ho sloupce matice $\boldsymbol{B}$, nebo ekvivalentně: $X(:,j) = \boldsymbol{A}.B(:,j)$.
b) $X(i,:) = \sum_{k=1}^{n} A(i,k).B(k,:)\ \forall i \ldots$ i-tý řádek X je lineární kombinací řádků matice $\boldsymbol{B}$ pomocí koeficientů z i-ho řádku matice $\boldsymbol{A}$, nebo ekvivalentně: $X(i,:) = A(i,:).\boldsymbol{B}$.

Hadamardův součin matic [`X = A .* B`]:

$$\underset{m\times n}{\boldsymbol{X}} = \underset{m\times n}{\boldsymbol{A}} \circ \underset{m\times n}{\boldsymbol{B}} \quad \overset{\text{def.}}{\equiv} \quad X(i,j) := A(i,j).B(i,j)\ \forall i,j.$$

Hadamardův součin je tedy operace součinu pro matice téhož typu zavedená po složkách podobně jako v případě sečítání.

Kroneckerův (přímý) součin matic [`X = kron(A,B)`]:

$$\underset{mm'\times nn'}{\boldsymbol{X}} = \underset{m\times n}{\boldsymbol{A}} \otimes \underset{m'\times n'}{\boldsymbol{B}} \quad \overset{\text{def.}}{\equiv} \quad \boldsymbol{X} = [A(i,j)\boldsymbol{B}]\ \forall i,j.$$

X je tedy matice sestavená z $m \times n$ bloků (submatic) $A(i,j)\boldsymbol{B}$ o rozměru $m' \times n'$.

Věta 4.14 (Vlastnosti multiplikativních operací).

(1) *Asociativita:*
$(\boldsymbol{A}.\boldsymbol{B}).\boldsymbol{C} = \boldsymbol{A}.(\boldsymbol{B}.\boldsymbol{C})$, $\quad (\boldsymbol{A} \circ \boldsymbol{B}) \circ \boldsymbol{C} = \boldsymbol{A} \circ (\boldsymbol{B} \circ \boldsymbol{C})$,
$(\boldsymbol{A} \otimes \boldsymbol{B}) \otimes \boldsymbol{C} = \boldsymbol{A} \otimes (\boldsymbol{B} \otimes \boldsymbol{C})$.

(2) *Distributivita zprava:*
$\boldsymbol{A}.(\boldsymbol{B}+\boldsymbol{C}) = \boldsymbol{A}.\boldsymbol{B}+\boldsymbol{A}.\boldsymbol{C}, \quad \boldsymbol{A}\circ(\boldsymbol{B}+\boldsymbol{C}) = \boldsymbol{A}\circ\boldsymbol{B}+\boldsymbol{A}\circ\boldsymbol{C},$
$\boldsymbol{A}\otimes(\boldsymbol{B}+\boldsymbol{C}) = \boldsymbol{A}\otimes\boldsymbol{B}+\boldsymbol{A}\otimes\boldsymbol{C}.$

(3) *Distributivita zleva:*
$(\boldsymbol{A}+\boldsymbol{B}).\boldsymbol{C} = \boldsymbol{A}.\boldsymbol{C}+\boldsymbol{B}.\boldsymbol{C}, \quad (\boldsymbol{A}+\boldsymbol{B})\circ\boldsymbol{C} = \boldsymbol{A}\circ\boldsymbol{C}+\boldsymbol{B}\circ\boldsymbol{C},$
$(\boldsymbol{A}+\boldsymbol{B})\otimes\boldsymbol{C} = \boldsymbol{A}\otimes\boldsymbol{C}+\boldsymbol{B}\otimes\boldsymbol{C}.$

(4) *Komutativita:*
$\boldsymbol{A}\circ\boldsymbol{B} = \boldsymbol{B}\circ\boldsymbol{A}.$
Maticový součin ani Kroneckerův součin nejsou obecně komutativní operace.

(5) *Jednotkový prvek:*
$\boldsymbol{I}_m.\boldsymbol{A} = \boldsymbol{A}.\boldsymbol{I}_n = \boldsymbol{A}, \quad \mathbf{1}_{m,n}\circ\boldsymbol{A} = \boldsymbol{A}\circ\mathbf{1}_{m,n} = \boldsymbol{A},$
$\mathbf{1}_{1,1}\otimes\boldsymbol{A} = \boldsymbol{A}\otimes\mathbf{1}_{1,1} = \boldsymbol{A}, \quad \boldsymbol{I}_n\otimes\boldsymbol{I}_m = \boldsymbol{I}_{mn}.$

(6) *(Hermitovská) transpozice součinu:*
$(\boldsymbol{A}.\boldsymbol{B})^T = \boldsymbol{B}^T.\boldsymbol{A}^T, \quad (\boldsymbol{A}.\boldsymbol{B})^* = \boldsymbol{B}^*.\boldsymbol{A}^*,$
$(\boldsymbol{A}\circ\boldsymbol{B})^T = \boldsymbol{A}^T\circ\boldsymbol{B}^T, \quad (\boldsymbol{A}\circ\boldsymbol{B})^* = \boldsymbol{A}^*\circ\boldsymbol{B}^*,$
$(\boldsymbol{A}\otimes\boldsymbol{B})^T = \boldsymbol{A}^T\otimes\boldsymbol{B}^T, \quad (\boldsymbol{A}\otimes\boldsymbol{B})^* = \boldsymbol{A}^*\otimes\boldsymbol{B}^*.$

(7) *Pravidlo smíšeného součinu:*
$(\boldsymbol{A}\otimes\boldsymbol{B}).(\boldsymbol{C}\otimes\boldsymbol{D}) = \boldsymbol{A}.\boldsymbol{C}\otimes\boldsymbol{B}.\boldsymbol{D}$ *pro matice kompatibilních rozměrů:*
$\boldsymbol{A}$ *je* $m\times n$, $\boldsymbol{C}$ *je* $n\times p$ $\Rightarrow$ $\boldsymbol{A}.\boldsymbol{C}$ *je* $m\times p$,
$\boldsymbol{B}$ *je* $m'\times n'$, $\boldsymbol{D}$ *je* $n'\times p'$ $\Rightarrow$ $\boldsymbol{B}.\boldsymbol{D}$ *je* $m'\times p'$,
Odtud: $\boldsymbol{A}\otimes\boldsymbol{B}$ *je* $(mm'\times nn')$ *a* $\boldsymbol{C}\otimes\boldsymbol{D}$ *je* $(nn'\times pp')$,
takže $(\boldsymbol{A}\otimes\boldsymbol{B}).(\boldsymbol{C}\otimes\boldsymbol{D})$ *má rozměr* $(mm'\times pp')$, *který je stejný jako rozměr matice* $\boldsymbol{A}.\boldsymbol{C}\otimes\boldsymbol{B}.\boldsymbol{D}$.

(8) *Maticový součin dvou vektorů:*
a) součin řádkového vektoru se sloupcovým:
$\boldsymbol{x} = [x_1;\dots;x_n], \boldsymbol{y} = [y_1;\dots;y_n] \Rightarrow \boldsymbol{x}^T\boldsymbol{y} = \boldsymbol{y}^T\boldsymbol{x} = \sum_{i=1}^n x_i y_i.$
b) součin sloupcového vektoru s řádkovým:
$\boldsymbol{x} = [x_1;\dots;x_m], \boldsymbol{y} = [y_1;\dots;y_n] \Rightarrow \boldsymbol{x}\boldsymbol{y}^T = [x_i y_j] \in \mathcal{M}_{m,n}.$

(9) *Skalární součiny pomocí maticového násobení* ($\mathbb{F}\subseteq\mathbb{C}$)*:*
$\boldsymbol{x} = [x_1;\dots;x_n], \boldsymbol{y} = [y_1;\dots;y_n] \Rightarrow \boldsymbol{y}^*\boldsymbol{x} = \sum_{i=1}^n x_i\overline{y}_i = \langle\boldsymbol{x},\boldsymbol{y}\rangle,$
$\boldsymbol{X} = [x_{ij}] \in \mathcal{M}_{n,p}, \boldsymbol{Y} = [y_{ij}] \in \mathcal{M}_{n,m} \Rightarrow \boldsymbol{Y}^*\boldsymbol{X} =: \boldsymbol{Z} \in \mathcal{M}_{m,p},$

kde $\boldsymbol{Z} =: [z_{ij}],\ z_{ij} = \langle X(:,j), Y(:,i)\rangle \overset{(S3)}{=} \overline{\langle Y(:,i), X(:,j)\rangle}\ \forall i,j.$
Tedy z_{ij} *je skalární součin* j*-ho sloupce matice* $\boldsymbol{X}$ *s* i*-tým sloupcem matice* $\boldsymbol{Y}$.
Speciálně pro $\boldsymbol{X} = \boldsymbol{Y} \in \mathcal{M}_{n,m}$ *je* $\boldsymbol{X}^*\boldsymbol{X} =: \boldsymbol{Z} \in \mathcal{M}_{m,m}$, *kde* $\boldsymbol{Z} =: [z_{ij}],\ z_{ij} = \langle X(:,j), X(:,i)\rangle \overset{(S3)}{=} \overline{\langle X(:,i), X(:,j)\rangle}\ \forall i,j.$
Matice $\boldsymbol{X}^*\boldsymbol{X}$ *je tzv.* **Gramova matice**.

(10) <u>*Součin s diagonální maticí:*</u> *Nechť* $\boldsymbol{D} = \operatorname{diag}(d_1,\ldots,d_m)$. *Pak* $\boldsymbol{A} =: [\boldsymbol{r}_1;\ldots;\boldsymbol{r}_m] \Rightarrow \boldsymbol{DA} = [d_1\boldsymbol{r}_1;\ldots;d_m\boldsymbol{r}_m]$ *a podobně* $\boldsymbol{A} =: [\boldsymbol{s}_1,\ldots,\boldsymbol{s}_m] \Rightarrow \boldsymbol{AD} = [d_1\boldsymbol{s}_1,\ldots,d_m\boldsymbol{s}_m]$. *Tedy vynásobení diagonální čtvercovou maticí zleva (zprava) vede k vynásobení řádků (sloupců) odpovídajícími diagonálními prvky.*

(11) <u>*Provedení permutace pomocí maticového násobení:*</u>
Nechť $\sigma : J \to J$ *je permutace transformující přirozeně uspořádanou množinu indexů* $J := \{1,\ldots,m\}$ *na permutovanou množinu* $\{\sigma(1),\ldots,\sigma(m)\}$ *a nechť* $\boldsymbol{P}_\sigma$ *je matice, která vznikne z jednotkové matice* I_n *stejnou permutací jejích řádků (řádek* $\sigma(i)$ *se přesune na* i*-tou pozici), tj.* $\boldsymbol{P}_\sigma := [\delta_{\sigma(i),j}]$. *Pak* $\boldsymbol{A} = [\boldsymbol{r}_1;\ldots;\boldsymbol{r}_m] \Rightarrow \boldsymbol{P}_\sigma.\boldsymbol{A} = [\boldsymbol{r}_{\sigma(1)};\ldots;\boldsymbol{r}_{\sigma(m)}]$ *a podobně* $\boldsymbol{A} = [\boldsymbol{s}_1,\ldots,\boldsymbol{s}_m] \Rightarrow \boldsymbol{A}.\boldsymbol{P}_\sigma^T = [\boldsymbol{s}_{\sigma(1)},\ldots,\boldsymbol{s}_{\sigma(m)}]$. *Tedy permutace řádků (sloupců) nějaké matice dosáhneme jejím vynásobením zleva (zprava) maticí, která vznikne z jednotkové matice provedením stejné permutace s jejími řádky (sloupci).*
Je-li $\boldsymbol{A} = \boldsymbol{D} = \operatorname{diag}(d_1,\ldots,d_m)$ *diagonální, pak složení téže řádkové a sloupcové permutace zřejmě stejným způsobem permutuje diagonálu v* $\boldsymbol{D}$*:* $\boldsymbol{P}_\sigma\boldsymbol{D}\boldsymbol{P}_\sigma^T = \operatorname{diag}(d_{\sigma(1)},\ldots,d_{\sigma(m)})$.

(12) <u>*Maticový součin dvou trojúhelníkových (diagonálních) matic:*</u>
Výsledkem maticového součinu dvou dolních (horních) trojúhelníkových matic je opět dolní (horní) trojúhelníková matice. Na diagonále jsou přitom součiny odpovídajích diagonálních prvků. Analogicky pro diagonální matice.

Důkaz. S výjimkou (7) jsou všechny vlastnosti bezprostředním důsledkem definic příslušných operací. □

4.3. **MATICE JAKO OPERÁTOR A HODNOST MATICE.**

Označení .
V konečně rozměrných vektorových prostorech lze báze vždy považovat za množiny lineárně uspořádané svými indexy. Vektory souřadnicového vyjádření operátoru $T : V_1 \to V_2$ z definice 3.35 ($\dim V_1 = n$, $\dim V_2 = m$, E_1 báze ve V_1, E_2 báze ve V_2) pak rovněž můžeme uspořádat jako sloupce v matici, tj. $[T]_{E_1,E_1} =: [[T\boldsymbol{e}_1]_{E_2}, \ldots, [T\boldsymbol{e}_n]_{E_2}]$ je pak maticí rozměru $m \times n$ nazývanou **maticovou reprezentací operátoru** T.
Nadále ve všech uvažovaných vektorových prostorech předpokládáme souřadnicové vyjádření v pevně zvolených a lineárně uspořádaných bázích, zejména pak v $(\mathbb{F}^n, \mathcal{L}_{\mathbb{F}})$ jimi budou přirozené báze $\mathcal{E}$, pokud nebude řečeno jinak. V souladu s definicemi 3.31 a 3.35 tedy budou vynechávány indexy jak ve vyjádření vektorů tak i operátorů: píšeme stručně $[\boldsymbol{x}]$ a $[T] = [[T\boldsymbol{e}_1], \ldots, [T\boldsymbol{e}_n]]$.

VĚTA 4.15. *Každá matice $\boldsymbol{T} \in \mathcal{M}_{m,n}$ určuje předpisem $\boldsymbol{x} \mapsto \boldsymbol{T}.\boldsymbol{x}$ ($\boldsymbol{x} \in \mathbb{F}^n$) tzv.* **maticový lineární operátor** $T : (\mathbb{F}^n, \mathcal{L}_{\mathbb{F}}) \to (\mathbb{F}^m, \mathcal{L}_{\mathbb{F}})$. *Přitom platí:*

(1) *Je-li $\boldsymbol{M} =: [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k]$ systém vektorů z $\mathbb{F}^n$ uspořádaný do sloupců matice, pak jeho obraz v operátoru T je matice* $T(\boldsymbol{M}) = [\boldsymbol{T}.\boldsymbol{x}_1, \ldots, \boldsymbol{T}.\boldsymbol{x}_k] \overset{4.13a)}{=} \boldsymbol{T}.\boldsymbol{M}$.
(2) $[T] = [[T\boldsymbol{\varepsilon}_1], \ldots, [T\boldsymbol{\varepsilon}_n]] = \boldsymbol{T}$.
(3) $\mathcal{R}(\boldsymbol{T}) := \mathcal{R}(T) = \mathcal{L}(\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n)$ *a* $\mathcal{R}(\boldsymbol{T}^T) = \mathcal{L}(\boldsymbol{r}_1, \ldots, \boldsymbol{r}_m)$, *kde $\boldsymbol{r}_i$ jsou řádky a $\boldsymbol{s}_j$ sloupce matice $\boldsymbol{T}$.*
(4) *Součinu dvou matic odpovídá složení příslušných maticových operátorů.*
(5) *Identická matice určuje identický operátor.*

Jestliže $\mathbb{F} \subseteq \mathbb{C}$, pak navíc platí:

(6) *Každá hermitovsky transponovaná matice $\boldsymbol{T}^*$ určuje operátor adjungovaný k operátoru určenému maticí $\boldsymbol{T}$, přičemž $\mathcal{R}(\boldsymbol{T}^*) = \mathcal{L}(\overline{\boldsymbol{r}}_1, \ldots, \overline{\boldsymbol{r}}_m)$. V případě reálné matice $\boldsymbol{T}$ hraje tutéž roli transponovaná matice $\boldsymbol{T}^T$.*

(7) *Operátor určený maticí $\boldsymbol{T}$ je samoadjungovaný právě když matice $\boldsymbol{T}$ je hermitovsky symetrická. V případě reálné matice $\boldsymbol{T}$ hraje tutéž roli symetrická matice.*

(8) *Matice $\boldsymbol{T}$ určuje unitárně izomorfní vnoření právě když její sloupce tvoří ortnormální množinu . Je-li $\boldsymbol{T}$ v takovém případě navíc čtvercová, pak určuje unitární operátor a nazývá se proto* **unitární maticí** *(resp.* **ortogonální maticí** *v případě $\mathbb{F} \subseteq \mathbb{R}$).*

DŮKAZ. K důkazu linearity stačí ověřit vlastnosti (1) a (2) z věty 3.27:
$\boldsymbol{T}.(\boldsymbol{x}+\boldsymbol{y}) = \boldsymbol{T}.\boldsymbol{x} + \boldsymbol{T}.\boldsymbol{y}$ je důsledkem distributivity 4.14(2).
$\boldsymbol{T}.(\alpha\boldsymbol{x}) = \alpha\boldsymbol{T}.\boldsymbol{x}$ plyne přímo z definice 4.13 maticového násobení: $\sum_{k=1}^{n} T(i,k)\alpha x_k = \alpha \sum_{k=1}^{n} T(i,k)x_k$.

(1) je opět přímým důsledkem maticového násobení dle 4.13a): totiž j-tý sloupec $T(\boldsymbol{M})$ je lineární kombinací sloupců $\boldsymbol{T}$ pomocí j-tého sloupce $M(:,j) = \boldsymbol{x}_j$, což je totéž jako $\boldsymbol{T}.\boldsymbol{x}_j$.

(2) $[T] = [[T\boldsymbol{\varepsilon}_1], \ldots, [T\boldsymbol{\varepsilon}_n]] \overset{4.4}{=} [T\boldsymbol{\varepsilon}_1, \ldots, T\boldsymbol{\varepsilon}_n] \overset{(1)}{=} \boldsymbol{T}.\boldsymbol{I}_n \overset{4.14(5)}{=} \boldsymbol{T}$.

(3) Podle 4.13a) je $\boldsymbol{T}.\boldsymbol{x}$ lineární kombinací sloupců $\boldsymbol{T}$ pomocí koeficientů vektoru $\boldsymbol{x} \in \mathbb{F}^n$. Pak $\mathcal{R}(\boldsymbol{T}) = \{\boldsymbol{T}.\boldsymbol{x} \mid \boldsymbol{x} \in \mathbb{F}^n\} \overset{3.12(2)}{=} \mathcal{L}(\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n)$. Podobně pro $\mathcal{R}(\boldsymbol{T}^T)$ a $\mathcal{R}(\boldsymbol{T}^*)$ v (6).

(4) je přímým důsledkem asociativity maticového násobení: $(\boldsymbol{U}.\boldsymbol{T}).\boldsymbol{x} \overset{4.14(1)}{=} \boldsymbol{U}.(\boldsymbol{T}.\boldsymbol{x})$.

(5) dle 4.14(5) platí $\boldsymbol{I}_n.\boldsymbol{x} = \boldsymbol{x}$ pro každé $\boldsymbol{x} \in \mathbb{F}^n$.

(6) $\langle \boldsymbol{T}.\boldsymbol{x}, \boldsymbol{y}\rangle \overset{4.14(9)}{=} \boldsymbol{y}^*.(\boldsymbol{T}.\boldsymbol{x}) \overset{4.14(1)}{=} (\boldsymbol{y}^*.\boldsymbol{T}).\boldsymbol{x} \overset{4.11(4)}{=} (\boldsymbol{y}^*.\boldsymbol{T}^{**}).\boldsymbol{x} =$

$\overset{4.14(6)}{=} (\boldsymbol{T}^*.\boldsymbol{y})^*.\boldsymbol{x} \overset{4.14(9)}{=} \langle \boldsymbol{x}, \boldsymbol{T}^*.\boldsymbol{y}\rangle$.
Je-li $\boldsymbol{T}$ reálná, pak $\boldsymbol{T}^* = \boldsymbol{T}^T$ dle 4.11(5).

(7) $\boldsymbol{T}$ určuje samoadjungovaný operátor $\overset{(6)}{\Leftrightarrow}$ $\boldsymbol{T} = \boldsymbol{T}^*$ $\overset{4.11(6)}{\Leftrightarrow}$ $\boldsymbol{T}$ je hermitovsky symetrická.

(8) • Nechť sloupce $\boldsymbol{T}$ jsou ortonormální. Podle (2) jsou obrazem ONB $\mathcal{E}$ a jelikož generují podprostor $\mathcal{R}(\boldsymbol{T})$ v $\mathbb{F}^m$, tak matice

$\boldsymbol{T}$ určuje unitárně izomorfní vnoření dle 3.89.

• Nechť naopak matice $\boldsymbol{T}$ určuje unitárně izomorfní vnoření. Pak její sloupce musí být jakožto obraz ONB $\mathcal{E}$ také ortonormální dle 3.91(2').

• Je-li $\boldsymbol{T}$ čtvercová, pak počet jejích sloupců je roven jejich délce m, která je dimenzí celého prostoru $\mathbb{F}^m$. Sloupce pak tvoří jeho bázi dle 3.24(4)(ii). $\boldsymbol{T}$ tedy určuje unitární operátor opět dle 3.89.

□

Poznámka 4.16. Podle věty 4.15 není tedy nadále třeba rozlišovat mezi maticí $\boldsymbol{T}$, příslušným lineárním operátorem T a jeho maticovou reprezentací $[T]$ v přirozené bázi. Poznamenejme však, že týž operátor může mít v jiné než přirozené bázi jinou maticovou reprezentaci. Naopak táž matice může v různých bázích reprezentovat různé operátory. Jak je ukázáno ve větě B.1 z přílohy B, mohou v tomto smyslu matice dokonce reprezentovat i lineární operátory mezi libovolnými abstraktními vektorovými prostory konečné dimenze.

DEFINICE 4.17 (HODNOST MATICE).
Sloupcovou (řádkovou) hodností matice $\boldsymbol{A} \in \mathcal{M}_{m,n}$, nazýváme dimenzi vektorového podprostoru $\mathcal{R}(\boldsymbol{A})$ v $\mathbb{F}^m$ ($\mathcal{R}(\boldsymbol{A}^T)$ v $\mathbb{F}^n$), což je dle 4.15(3) právě podprostor generovaný sloupci (řádky) matice $\boldsymbol{A}$. Podle níže dokázané věty 4.23 je sloupcová i řádková hodnost stejná, nazývá se **hodností matice $\boldsymbol{A}$** a značí se $\mathrm{r}(\boldsymbol{A})$. Matice $\boldsymbol{A}$ se nazývá **maticí sloupcově (řádkově) plné hodnosti**, jestliže $\mathrm{r}(\boldsymbol{A}) = n$ ($\mathrm{r}(\boldsymbol{A}) = m$).
Matice A se nazývá **regulární**[15], je-li současně řádkově i sloupcově plné hodnosti. Čtvercová matice, která není regulární se nazývá **singulární**.

---

[15]Regulární matice musí být čtvercová, neboť počet lineárně nezávislých sloupců n nemůže přesáhnout dimenzi prostoru $\mathbb{F}^m$, tj. musí platit $n \leq m$. Analogicky z lineární nezávislosti řádků dostáváme $m \leq n$.

Poznámka 4.18. S ohledem na větu 3.19 a její důsledek 3.20 udává sloupcová (řádková) hodnost matice počet prvků libovolné báze (neboli maximální lineárně nezávislé podmnožiny) vybrané z generující množiny všech jejích sloupců (řádků). Zejména tedy:

a) Matice je sloupcově (řádkově) plné hodnosti právě když všechny její sloupce (řádky) jsou lineárně nezávislé.
b) Matice je regulární právě když je čtvercová a má lineárně nezávislé všechny řádky i sloupce[15].

V dalším se zaměříme na důkaz tvrzení o shodnosti sloupcové a řádkové hodnosti matice. Zde budou klíčovou roli hrát takové transformace dané matice, které zachovají beze změny její sloupcovou i řádkovou hodnost. Dále budeme psát $\boldsymbol{A} \sim \boldsymbol{B}$, pokud matice $\boldsymbol{A}$ a $\boldsymbol{B}$ mají shodné sloupcové i řádkové hodnosti. Takto zavedená relace je zřejmě ekvivalencí na množině všech matic nad týmž skalárním polem $\mathbb{F}$.

VĚTA 4.19.

(1) *Každá regulární matice má stejnou sloupcovou a řádkovou hodnost.*
(2) $\boldsymbol{A}$ *je regulární právě když* $\boldsymbol{A}^T$ *je regulární.*
(3) *Nechť* $A([i_1,\ldots,i_r],[j_1,\ldots,j_r])$ *je regulární submatice řádu* r *matice* $\boldsymbol{A}$ *typu* m/n. *Pak sloupce* $A(:,j_1),\ldots,A(:,j_r)$ *i řádky* $A(i_1,:),\ldots,A(i_r,:)$ *jsou lineárně nezávislé.*
(4) *Jednotková matice je regulární.*

DŮKAZ.

(1) Dle 4.18b) má regulární matice stejný počet řádků (=řádková hodnost) i sloupců (=sloupcová hodnost).
(2) Tvrzení je opět důsledkem 4.18b), neboť $\boldsymbol{A}^T$ vznikne z $\boldsymbol{A}$ záměnou řádků za sloupce a naopak.
(3) $\sum_{k=1}^{r} \alpha_k A(:,j_k) = \mathbf{0}_{m,1} \Rightarrow \sum_{k=1}^{r} \alpha_k A([i_1,\ldots,i_r],j_k) = \mathbf{0}_{r,1} \Rightarrow \alpha_1 = 0,\ldots,\alpha_r = 0$ dle 4.18b). Nezávislost řádků se dokáže podobně.
(4) Řádky i sloupce jednotkové matice jsou prvky přirozené báze a tudíž jsou lineárně nezávislé.

$\square$

VĚTA 4.20.

(1) *Matice $\boldsymbol{A}$ je sloupcově plné hodnosti právě když příslušný maticový operátor je izomorfní vnoření.*
(2) *Matice $\boldsymbol{A}$ je řádkově plné hodnosti právě když příslušný maticový operátor je surjektivní.*
(3) *Matice $\boldsymbol{A}$ je regulární právě když příslušný maticový operátor je izomorfizmus.*

DŮKAZ.

(1) Matice $\boldsymbol{A}$ typu m/n je sloupcově plné hodnosti $\overset{4.18a)}{\Leftrightarrow}$ její sloupce jsou lineárně nezávislé $\overset{4.13a)}{\Leftrightarrow}$ $[\boldsymbol{A}.\boldsymbol{x} = 0 \Rightarrow \boldsymbol{x} = \boldsymbol{0}]$ $\Leftrightarrow$ $\mathcal{N}(\boldsymbol{A}) = \{\boldsymbol{0}\}$ $\overset{3.30(1)}{\Leftrightarrow}$ $\boldsymbol{A}$ určuje izomorfní vnoření.
(2) Ukážeme ekvivalenci negovaných výroků (viz 1.1(6)):
Matice $\boldsymbol{A}$ typu m/n není řádkově plné hodnosti $\Leftrightarrow$ $\boldsymbol{A}^T$ nemá lineárně nezávislé sloupce $\Leftrightarrow$ $\boldsymbol{A}^*$ nemá lineárně nezávislé sloupce (srov. důkaz 4.23) $\Leftrightarrow$ matice $\boldsymbol{A}^*$ typu n/m není sloupcově plné hodnosti $\overset{(1)}{\Leftrightarrow}$ maticový operátor příslušný k $\boldsymbol{A}^*$ není izomorfní vnoření $\overset{3.30(1)}{\Leftrightarrow}$ $\exists\, \boldsymbol{0} \neq \boldsymbol{y} \in \mathbb{F}^m : \boldsymbol{A}^*\boldsymbol{y} = \boldsymbol{0}$ $\overset{3.58(S4)}{\Leftrightarrow}$ $\exists\, \boldsymbol{0} \neq \boldsymbol{y} \in \mathbb{F}^m : \langle \boldsymbol{A}^*\boldsymbol{y}, \boldsymbol{A}^*\boldsymbol{y}\rangle = 0$ $\Leftrightarrow$ $\exists\, \boldsymbol{0} \neq \boldsymbol{y} \in \mathbb{F}^m$: $\langle \boldsymbol{A}\boldsymbol{x}, \boldsymbol{y}\rangle \overset{3.82,4.15(6)}{=} \langle \boldsymbol{x}, \boldsymbol{A}^*\boldsymbol{y}\rangle = 0\, \forall\, \boldsymbol{x} \in \mathbb{F}^n$ $\Leftrightarrow$ $\exists\, \boldsymbol{0} \neq \boldsymbol{y} \in \mathcal{R}(A)^\perp$ $\Leftrightarrow$ $\exists\, \boldsymbol{z} \in \mathbb{R}^m - \mathcal{R}(\boldsymbol{A}) : \boldsymbol{z} = P_{\mathcal{R}(\boldsymbol{A})}\boldsymbol{z} + \boldsymbol{y}$ (bez újmy na obecnosti lze za $\boldsymbol{z}$ zvolit rovnou $\boldsymbol{0} \neq \boldsymbol{y} \in \mathcal{R}(\boldsymbol{A})^\perp$) $\Leftrightarrow$ maticový operátor příslušný k $\boldsymbol{A}$ není surjektivní.
(3) Matice $\boldsymbol{A}$ je regulární $\overset{4.17}{\Leftrightarrow}$ je současně sloupcově i řádkově plné hodnosti $\overset{(1),(2)}{\Leftrightarrow}$ $\boldsymbol{A}$ určuje surjektivní izomorfní vnoření $\Leftrightarrow$ $\boldsymbol{A}$ určuje izomorfizmus.

$\square$

LEMMA 4.21.
Sloupcová ani řádková hodnost matice se nemění při jejím násobení zleva (zprava) maticí sloupcově (řádkově) plné hodnosti.

DŮKAZ. Nechť $\boldsymbol{R} \in \mathcal{M}_{p,m}$ je matice sloupcově plné hodnosti m a $\boldsymbol{A}$ nějaká matice typu m/n. Pak

a) $\mathcal{R}(\boldsymbol{R}.\boldsymbol{A}) = \{\boldsymbol{R}.(\boldsymbol{A}.\boldsymbol{x}) \,|\, \boldsymbol{x} \in \mathbb{F}^n\} = \{\boldsymbol{R}.\boldsymbol{y} \,|\, \boldsymbol{y} \in \mathcal{R}(\boldsymbol{A})\} \overset{4.20(1)}{\Rightarrow}$ $\mathcal{R}(\boldsymbol{R}.\boldsymbol{A})$ je izomorfním obrazem podprostoru $\mathcal{R}(\boldsymbol{A}) \overset{3.33}{\Rightarrow}$ $\dim \mathcal{R}(\boldsymbol{R}.\boldsymbol{A}) = \dim \mathcal{R}(\boldsymbol{A}) \Rightarrow$ matice $\boldsymbol{R}.\boldsymbol{A}$ a $\boldsymbol{A}$ mají stejnou sloupcovou hodnost.

b) $\boldsymbol{R}^T$ je řádkově plné hodnosti $\overset{4.20(2)}{\Rightarrow}$ $\boldsymbol{R}^T$ je surjekce $\Rightarrow$ $\mathcal{R}((\boldsymbol{R}.\boldsymbol{A})^T) \overset{4.14(6)}{=} \mathcal{R}(\boldsymbol{A}^T.\boldsymbol{R}^T) = \{\boldsymbol{A}^T.(\boldsymbol{R}^T.\boldsymbol{x}) \,|\, \boldsymbol{x} \in \mathbb{F}^p\} = \{\boldsymbol{A}^T.\boldsymbol{y} \,|\, \boldsymbol{y} \in \mathcal{R}(\boldsymbol{R}^T) = \mathbb{F}^m\} = \mathcal{R}(\boldsymbol{A}^T) \Rightarrow \dim \mathcal{R}((\boldsymbol{R}.\boldsymbol{A})^T) = \dim \mathcal{R}(\boldsymbol{A}^T) \overset{4.17}{\Rightarrow}$ matice $\boldsymbol{R}.\boldsymbol{A}$ a $\boldsymbol{A}$ mají stejnou řádkovou hodnost.

Násobení zprava maticí řádkově plné hodnosti lze transpozicí převést na násobení zleva maticí sloupcově plné hodnosti: $(\boldsymbol{A}.\boldsymbol{R})^T = \boldsymbol{R}^T.\boldsymbol{A}^T$. Dle předcházející části mají $(\boldsymbol{A}.\boldsymbol{R})^T$ a $\boldsymbol{A}^T$ stejnou řádkovou i sloupcovou hodnost a tedy totéž musí platit i pro $\boldsymbol{A}.\boldsymbol{R}$ a $\boldsymbol{A}$. □

VĚTA 4.22 (Skeletní rozklad matice)**.**
Nechť $\boldsymbol{A}$ je nenulová matice typu m/n sloupcové hodnosti r, pak existuje matice sloupcově plné hodnosti $\boldsymbol{B}$ typu m/r a matice řádkově plné hodnosti $\boldsymbol{C}$ typu r/n tak, že $\boldsymbol{A} = \boldsymbol{B}.\boldsymbol{C}$. Přitom $\boldsymbol{C}$ má stejnou řádkovou i sloupcovou hodnost r a platí $\mathcal{R}(\boldsymbol{A}) = \mathcal{R}(\boldsymbol{B})$, $\mathcal{R}(\boldsymbol{A}^T) = \mathcal{R}(\boldsymbol{C}^T)$ a $\mathcal{N}(\boldsymbol{A}) = \mathcal{N}(\boldsymbol{C})$. Přitom $\boldsymbol{C}$ lze zvolit tak, aby $\boldsymbol{I}_r$ byla její submaticí.

DŮKAZ. Položme $\boldsymbol{B} := A(:,[j_1,\ldots,j_r])$ rovno submatici v $\boldsymbol{A}$ sestávající z vhodně vybraných sloupců tvořících bázi v $\mathcal{R}(\boldsymbol{A})$. Takový výběr je vždy možný dle 3.20. Tyto sloupce jsou lineárně nezávislé, takže $\boldsymbol{B}$ je dle 4.18a) sloupcově plné hodnosti a přitom $\mathcal{R}(\boldsymbol{A}) = \mathcal{R}(\boldsymbol{B})$. Každý sloupec matice $\boldsymbol{A}$ patří do $\mathcal{R}(\boldsymbol{A})$, takže musí být nějakou lineární kombinací bázových sloupců z $\boldsymbol{B}$. Nechť $\boldsymbol{C}$ je matice, jejíž j-tý

sloupec $C(:,j)$ je příslušný vektor souřadnic j-tého sloupec matice $\boldsymbol{A}$ v bázi $\boldsymbol{B}$. Na základě 4.13a) tedy můžeme psát $\boldsymbol{A} = \boldsymbol{B}.\boldsymbol{C}$. Vektorem souřadnic k-tého bázového sloupce $A(:,j_k)$ je ε_k $(k = 1,\dots,r)$, což znamená, že jednotková matice $\boldsymbol{I}_r = C(:,[j_1,\dots,j_r])$ je submaticí matice $\boldsymbol{C}$. Jelikož $\boldsymbol{I}_r$ je dle 4.19(4) regulární, jsou podle 4.19(3) lineárně nezávislé jak všechny řádky matice $\boldsymbol{C}$ (tj. $\boldsymbol{C}$ je řádkově plné hodnosti), tak i sloupce $C(:,j_1),\dots,C(:,j_r)$. Ty dokonce tvoří bázi v $\mathcal{R}(\boldsymbol{C}) = \mathbb{F}^r$, neboť $\dim \mathbb{F}^r = r$ (viz 3.24(4)(ii)). Tedy r je nejen řádková, ale i sloupcová hodnost matice $\boldsymbol{C}$.
V části b) důkazu lemmatu 4.21 jsme ukázali $\mathcal{R}(\boldsymbol{A}^T) = \mathcal{R}((\boldsymbol{B}.\boldsymbol{C})^T) = \mathcal{R}(\boldsymbol{C}^T)$. Platí také $\mathcal{N}(\boldsymbol{A}) = \mathcal{N}(\boldsymbol{C})$: $\boldsymbol{B}$ určuje dle 4.20(1) izomorfní vnoření, takže $\mathcal{N}(\boldsymbol{B}) \overset{3.30(1)}{=} \{\boldsymbol{0}\}$ a platí $\boldsymbol{x} \in \mathcal{N}(\boldsymbol{A}) \;\Leftrightarrow\; \boldsymbol{0} = \boldsymbol{A}.\boldsymbol{x} = \boldsymbol{B}.(\boldsymbol{C}.\boldsymbol{x}) \;\Leftrightarrow\; \boldsymbol{C}.\boldsymbol{x} \in \mathcal{N}(\boldsymbol{B}) = \{\boldsymbol{0}\} \;\Leftrightarrow\; \boldsymbol{0} = \boldsymbol{C}.\boldsymbol{x} \;\Leftrightarrow \boldsymbol{x} \in \mathcal{N}(\boldsymbol{C})$. □

<u>VĚTA</u> 4.23 (Tvrzení o shodě řádkové a sloupcové hodnosti).
Každá matice $\boldsymbol{A}$ má stejnou řádkovou i sloupcovou hodnost, neboli $\dim \mathcal{R}(\boldsymbol{A}) = \dim \mathcal{R}(\boldsymbol{A}^T)$. *Zejména platí* $\mathrm{r}(\boldsymbol{A}) = \mathrm{r}(\boldsymbol{A}^T)$. *V případě* $\mathbb{F} \subseteq \mathbb{C}$ *platí také* $\mathrm{r}(\boldsymbol{A}) = \mathrm{r}(\boldsymbol{A}^*)$.

DŮKAZ.
Nechť $\boldsymbol{A} = \boldsymbol{B}.\boldsymbol{C}$ je skeletní rozklad matice $\boldsymbol{A}$. Pak $\boldsymbol{A} \sim \boldsymbol{C}$ dle 4.21. Tedy matice $\boldsymbol{A}$ má stejnou řádkovou i sloupcovou hodnost jako $\boldsymbol{C}$. Ta má však obě hodnosti stejné, takže totéž musí platit pro $\boldsymbol{A}$.
V případě $\mathbb{F} \subseteq \mathbb{C}$ rovnost $h := \mathrm{r}(\boldsymbol{A}) = \mathrm{r}(\boldsymbol{A}^*)$ plyne z 3.88(5)(iv). Dá se ale dokázat i přímo jako důsledek faktu, že operace komplexního sdružení zachovává lineární nezávislost: totiž značí-li $\boldsymbol{r}_i$ například řádky matice $\boldsymbol{A}$ pak $\overline{\boldsymbol{r}}_i$ jsou sloupce matice $\boldsymbol{A}^*$. Přitom $\sum_{j=1}^k \alpha_j \boldsymbol{r}_{i_j} = \boldsymbol{0} = \overline{\boldsymbol{0}} = \sum_{j=1}^k \overline{\alpha}_j \overline{\boldsymbol{r}}_{i_j}$, kde $\alpha_j = 0 \;\Leftrightarrow\; \overline{\alpha}_j = 0$. V důsledku toho je $\boldsymbol{r}_{i_1},\dots,\boldsymbol{r}_{i_h}$ maximální lineárně nezávislá mezi všemi řádky $\boldsymbol{A}$ právě když $\overline{\boldsymbol{r}}_{i_1},\dots,\overline{\boldsymbol{r}}_{i_h}$ je maximální lineárně nezávislá mezi všemi komplexně sdruženými řádky matice $\boldsymbol{A}$, tj. mezi všemi sloupci matice $\boldsymbol{A}^*$.
□

VĚTA 4.24 (Řádkové/sloupcové úpravy zachovávající hodnost).

(1) *Hodnost matice se nemění při jejím násobení zleva (zprava) maticí sloupcově (řádkově) plné hodnosti.*
(2) *Součin dvou matic sloupcově (řádkově) plné hodnosti je opět matice sloupcově (řádkově) plné hodnosti.*
(3) *Hodnost matice se nemění při jejím násobení zleva nebo zprava regulární maticí.*
(4) *Součin regulárních matic je regulární matice.*
(5) *Hodnost matice se nemění permutací jejích sloupců nebo řádků.*
(6) *Hodnost matice se nemění vynecháním sloupce (řádku), který je lineární kombinací ostatních sloupců (řádků).*
(7) *Hodnost matice se nemění vynásobením některého sloupce nebo řádku nenulovým skalárem.*
(8) *Hodnost matice se nemění přičtením skalárního násobku některých sloupců (řádků) k jinému sloupci (řádku).*
(9) *Hodnost matice se nemění vynecháním nulových sloupců nebo řádků.*

DŮKAZ. Vzhledem k 4.23 všechny úvahy prováděné dále se sloupci platí i pro řádky a naopak. Tvrzení (1) již bylo dokázáno v lemmatu 4.21. Tvrzení (2) je speciálním případem (1) stejně jako (3), neboť regulární matice má plnou sloupcovou i řádkovou hodnost. Podobně (4) je důsledkem (3). Tvrzení (2) a (4) lze jinou úvahou odvodit také z věty 4.20: totiž součinu matic sloupcově (řádkově) plné hodnosti, resp. regulárních, odpovídá dle 4.15(4) složení dvou izomorfních vnoření (surjektivních lineárních zobrazení), resp. izomorfizmů, což je opět lineární zobrazení téhož typu.
Tvrzení (5) je zřejmé, neboť prostor generovaný řádky nebo sloupci (a tedy ani jeho dimenze) nezávisí na uspořádání množiny generátorů. Tvrzení (6)–(8) jsou elementární úpravy z věty 3.14, které rovněž nemění generovaný podprostor a tedy ani jeho dimenzi. Tvrzení (9) je speciálním případem (6), neboť každý nulový sloupec či řádek lze považovat za nulovou lineární kombinaci ostatních sloupců (řádků). □

<u>VĚTA</u> 4.25.
Čtvercová matice $\boldsymbol{A}$ řádu n je regulární právě když existují čtvercové matice $\boldsymbol{A}_1$, $\boldsymbol{A}_2$ řádu n takové, že $\boldsymbol{A}_1.\boldsymbol{A} = \boldsymbol{A}.\boldsymbol{A}_2 = \boldsymbol{I}_n$. V takovém případě $\boldsymbol{A}_1 = \boldsymbol{A}_2 =: \boldsymbol{A}^{-1}$ je jediná, je regulární a určuje maticový operátor inverzní k operátoru určenému maticí $\boldsymbol{A}$. Matici $\boldsymbol{A}^{-1}$ nazýváme **maticí inverzní k $\boldsymbol{A}$** [v MATLABu: `inv(A)`].

DŮKAZ. $\boldsymbol{A}$ je regulární $\overset{4.20(3)}{\Leftrightarrow}$ $\boldsymbol{A}$ určuje izomorfizmus.
• Jestliže $\boldsymbol{A}$ určuje izomorfizmus, nechť $\boldsymbol{A}^{-1}$ je maticová reprezenatce inverzního operátoru. Pak $\boldsymbol{A}^{-1}.\boldsymbol{A} = \boldsymbol{A}.\boldsymbol{A}^{-1} = \boldsymbol{I}_n$ dle 4.15(4)(5).
• Nechť platí $\boldsymbol{A}_1.\boldsymbol{A} = \boldsymbol{A}.\boldsymbol{A}_2 = \boldsymbol{I}_n$. Protože identický operátor $\boldsymbol{I}_n$ je prosté a surjektivní zobrazení, platí: $\boldsymbol{A}.\boldsymbol{x} = \boldsymbol{A}.\boldsymbol{y} \Rightarrow \boldsymbol{A}_1.\boldsymbol{A}.\boldsymbol{x} = \boldsymbol{A}_1.\boldsymbol{A}.\boldsymbol{y} \Rightarrow \boldsymbol{I}_n.\boldsymbol{x} = \boldsymbol{I}_n.\boldsymbol{y} \Rightarrow \boldsymbol{x} = \boldsymbol{y} \Rightarrow \boldsymbol{A}$ je prosté.
Podobně pro každé $\boldsymbol{y}$ máme $\boldsymbol{y} = \boldsymbol{I}_n.\boldsymbol{y} = \boldsymbol{A}.\boldsymbol{A}_2.\boldsymbol{y} \in \mathcal{R}(\boldsymbol{A}) \Rightarrow \boldsymbol{A}$ je také surjektivní. Celkem $\boldsymbol{A}$ je tedy izomorfizmus. Přitom $\boldsymbol{A}_2 = \boldsymbol{I}_n.\boldsymbol{A}_2 = \boldsymbol{A}_1.\boldsymbol{A}.\boldsymbol{A}_2 = \boldsymbol{A}_1.\boldsymbol{I}_n = \boldsymbol{A}_1$. Po záměně role $\boldsymbol{A}$ a $\boldsymbol{A}^{-1}$ vidíme, že $\boldsymbol{A}^{-1}$ je rovněž regulární a určuje izomorfizmus inverzní k izomorfizmu určenému maticí $\boldsymbol{A}$. $\square$

<u>VĚTA</u> 4.26. *Každá permutační matice $\boldsymbol{P}_\sigma$ je regulární a v případě $\mathbb{F} \subseteq \mathbb{C}$ je dokonce unitární.*

<u>DŮKAZ</u>. $\boldsymbol{P}_\sigma$ řádu n je regulární na základě věty 4.24(5), neboť je dle 4.14(11) permutací řádků jednotkové matice $\boldsymbol{I}_n$, která je regulární dle 4.19(4). V případě $\mathbb{F} \subseteq \mathbb{C}$ unitárnost matice $\boldsymbol{P}_\sigma$ pak plyne z 3.90(3): $\langle \boldsymbol{P}_\sigma.\boldsymbol{x}, \boldsymbol{P}_\sigma.\boldsymbol{y} \rangle \overset{4.14(9)}{=} \sum_{i=1}^n x_{\sigma(i)} \overline{y}_{\sigma(i)} = \sum_{i=1}^n x_i \overline{y}_i \overset{4.14(9)}{=} \langle \boldsymbol{x}, \boldsymbol{y} \rangle$, neboť sečítání je komutativní a nezávisí tedy na permutaci sčítanců. $\square$

<u>VĚTA</u> 4.27. *Čtvercová trojúhelníková (diagonální) matice je regulární právě když všechny její prvky na hlavní diagonále jsou nenulové.*

Důkaz. Vzhledem k 4.19(2) a 4.11(8) stačí tvrzení ověřit například pro horní trojúhelníkovou matici $\boldsymbol{A}$ řádu n.
• Nechť $a_{ii} \neq 0$ pro každé $i = 1, \ldots, n$. Dle 4.18b) a 4.23 stačí ukázat například jen lineární nezávislost řádků. Z rovnosti $[0, \ldots, 0] =$

$\sum_{i=1}^{n} \alpha_i A(i,:)$ postupně dostáváme:
$0 = \alpha_1 a_{11}$, $0 = \alpha_1 a_{12} + \alpha_2 a_{22}, \ldots, 0 = \sum_{k=1}^{n-1} \alpha_k a_{kn} + \alpha_n a_{nn}$.
Z 1. rovnice $a_{11} \neq 0 \Rightarrow \alpha_1 = 0$, po dosazení do 2. rovnice analogicky $a_{22} \neq 0 \Rightarrow \alpha_2 = 0$, atd. až z poslední rovnice $a_{nn} \neq 0 \Rightarrow \alpha_n = 0$.
• Předpokládejme, že $a_{ii} = 0$ pro nějaké i. Vezměme nejmenší takové i. Je-li $i = 1$, pak 1. sloupec je nulový a $\boldsymbol{A}$ tedy není regulární. Je-li $i > 1$, pak $A([1,\ldots,i-1],[1,\ldots,i-1])$ je horní trojúhelníková submatice řádu $i-1$ s nenulovou diagonálou a tudíž regulární dle předchozí části. Dle 4.19(3) jsou nezávislé celé sloupce $A(:,1),\ldots,A(:,i-1)$ a protože $A([i,\ldots,n],[1,\ldots,i])$ je nulová submatice v důsledku $a_{ii} = 0$, je sloupec $A(:,i)$ lineární kombinací prvých $i-1$ sloupců, tj. sloupce $\boldsymbol{A}$ jsou závislé a $\boldsymbol{A}$ opět nemůže být regulární.
Diagonální matice je speciálním případem trojúhelníkové matice. □

<u>DŮSLEDEK</u> 4.28 (Vlastnosti inverzních matic)**.**
Nechť $\boldsymbol{A}$, $\boldsymbol{B}$ jsou dvě čtvercové matice řádu n. Pak

(1) *$\boldsymbol{A}$ je regulární právě když $\boldsymbol{A}^T$ je regulární. V takovém případě platí $(\boldsymbol{A}^T)^{-1} = (\boldsymbol{A}^{-1})^T$.*
(1') *V případě $\mathbb{F} \subseteq \mathbb{C}$ je obdobně $\boldsymbol{A}$ regulární právě když $\boldsymbol{A}^*$ je regulární. V takovém případě platí $(\boldsymbol{A}^*)^{-1} = (\boldsymbol{A}^{-1})^*$.*
(2) *$\boldsymbol{A}$, $\boldsymbol{B}$ regulární $\Rightarrow (\boldsymbol{A}.\boldsymbol{B})^{-1} = \boldsymbol{B}^{-1}.\boldsymbol{A}^{-1}$.*
(3) *Je-li $\boldsymbol{P}_\sigma$ permutační matice určená permutací σ dle 4.14(11), pak $\boldsymbol{P}_{\sigma^{-1}} = \boldsymbol{P}_\sigma^{-1} = \boldsymbol{P}_\sigma^T$.*
(4) *Je-li $\boldsymbol{A} =: [a_{ij}]$ regulární dolní (horní) trojúhelníková matice řádu n, pak $\boldsymbol{A}^{-1}$ je rovněž dolní (horní) trojúhelníková matice s prvky $a_{11}^{-1},\ldots,a_{nn}^{-1}$ na hlavní diagonále. Je-li $\boldsymbol{A}$ dokonce diagonální, pak $\boldsymbol{A}^{-1}$ je rovněž diagonální.*

Důkaz.

(1) $\boldsymbol{A}^T$ regulární $\overset{4.19(2)}{\Leftrightarrow}$ $\boldsymbol{A}$ je regulární $\overset{4.25}{\Leftrightarrow}$ $\boldsymbol{A}^{-1}.\boldsymbol{A} = \boldsymbol{A}.\boldsymbol{A}^{-1} = \boldsymbol{I}_n \overset{4.14(6)}{\Leftrightarrow} \boldsymbol{A}^T.(\boldsymbol{A}^{-1})^T = (\boldsymbol{A}^{-1})^T.\boldsymbol{A}^T = \boldsymbol{I}_n^T \overset{4.11(7)}{=} \boldsymbol{I}_n \overset{4.25}{\Leftrightarrow} (\boldsymbol{A}^T)^{-1} = (\boldsymbol{A}^{-1})^T$.

(1') Pro A^* se ukáže podobně. S ohledem na 4.15(6) plyne také přímo z 3.88(5)(vi).

(2) Plyne z toho, že inverzní zobrazení se skládají v opačném pořadí. Jiné odvození se opět může opírat o větu 4.25: $\boldsymbol{B}^{-1}.\boldsymbol{A}^{-1}.\boldsymbol{A}.\boldsymbol{B} = \boldsymbol{B}^{-1}.\boldsymbol{B} = \boldsymbol{I}_n$ a analogicky $\boldsymbol{A}.\boldsymbol{B}.\boldsymbol{B}^{-1}.\boldsymbol{A}^{-1} = \boldsymbol{A}.\boldsymbol{A}^{-1} = \boldsymbol{I}_n$.

(3) Dle 4.14(11): $\boldsymbol{P}_\sigma = [\delta_{\sigma(i),j}] \Rightarrow \boldsymbol{P}_\sigma^T = [\delta_{j,\sigma(i)}] = [\delta_{\sigma^{-1}(j),i}]$, neboť $j = \sigma(i)$ právě když $\sigma^{-1}(j) = \sigma^{-1}(\sigma(i)) = i$. Matice $\boldsymbol{P}_\sigma^T$ tedy reprezentuje operátor inverzní permutace σ^{-1}, tj. $\boldsymbol{P}_{\sigma^{-1}} = \boldsymbol{P}_\sigma^T$. Vezmeme-li v 4.14(11) za diagonální matici jednotkovou matici $\boldsymbol{D} = \boldsymbol{I}_n$, pak $\boldsymbol{D}$ se nezmění při permutaci samých jedniček na diagonále. Platí tedy $\boldsymbol{P}_\sigma.\boldsymbol{P}_\sigma^T = \boldsymbol{P}_\sigma.\boldsymbol{I}_n.\boldsymbol{P}_\sigma^T = \boldsymbol{I}_n$ a po záměně σ za σ^{-1} si matice $\boldsymbol{P}$ a $\boldsymbol{P}^T$ rovněž zamění roli, takže také platí $\boldsymbol{P}_\sigma^T.\boldsymbol{P}_\sigma = \boldsymbol{I}_n$ a $\boldsymbol{P}_\sigma^{-1} \overset{4.25}{=} \boldsymbol{P}_\sigma^T$.

(4) Nechť $\boldsymbol{A} =: [a_{ij}]$ je například dolní trojúhelníková regulární matice řádu n. Dle 4.27 jsou $a_{ii} \neq 0$ pro $i = 1, \ldots, n$. Podle 4.25 musí pro matici $\boldsymbol{X} =: [x_{j,k}]$ inverzní k $\boldsymbol{A}$ platit $\boldsymbol{I}_n = \boldsymbol{A}.\boldsymbol{X}$. Srovnáváním naddiagonálových prvků v i-tém řádku a k-tém sloupci na levé a pravé straně této rovnice dostáváme postupně pro $i = 1, \ldots, n$ a $k \geq i$:
$\delta_{1k} = \sum_{j=1}^n a_{1j}x_{jk} = a_{11}x_{1k} \Rightarrow 1 = a_{11}x_{11}$ a $0 = a_{11}x_{1k}$ pro $k > 1 \Rightarrow x_{11} = a_{11}^{-1}$ a $x_{1k} = 0$ pro $k > 1$. Analogicky pro $i = 2$: $\delta_{2k} = \sum_{j=1}^n a_{2j}x_{jk} = a_{21}x_{1k} + a_{22}x_{2k} = a_{22}x_{2k} \Rightarrow x_{22} = a_{22}^{-1}$ a $x_{2k} = 0$ pro $k > 2$, atd.
Případ horní trojúhelníkové matice převedeme na předchozí situaci transpozicí užitím 4.11(8) a 4.14(6): Podle 4.25 musí také platit $\boldsymbol{I}_n = \boldsymbol{X}.\boldsymbol{A}$, odtud $\boldsymbol{I}_n = \boldsymbol{I}_n^T = (\boldsymbol{X}.\boldsymbol{A})^T = \boldsymbol{A}^T.\boldsymbol{X}^T$, kde $\boldsymbol{A}^T$ je dolní trojúhelníková, takže dle předchozí části je také $\boldsymbol{X}^T$ dolní trojúhelníková a tedy $\boldsymbol{X}$ horní trojúhelníková. Diagonálové prvky se transpozicí také nemění.
Matice $\boldsymbol{A}$ je diagonální právě když je současně horní i dolní trojúhelníková, takže její inverze musí také mít obě vlastnosti, tj. musí být diagonální.

$\square$

<u>VĚTA</u> 4.29 (Zjišťování hodnosti)**.**
Nechť $\boldsymbol{A}$ je matice typu m/n a $\boldsymbol{B}$ typu n/p. Pak platí:

(1) $\mathrm{r}(\boldsymbol{A}) \leq \min(m, n)$.
(2) $\mathrm{r}(\boldsymbol{A}.\boldsymbol{B}) \leq \min(\mathrm{r}(\boldsymbol{A}), \mathrm{r}(\boldsymbol{B}))$. *Je-li $\boldsymbol{A}$ sloupcově plné hodnosti, resp. $\boldsymbol{B}$ řádkově plné hodnosti, pak nastane rovnost a* $\mathrm{r}(\boldsymbol{A}.\boldsymbol{B}) = \mathrm{r}(\boldsymbol{B})$, *resp.* $\mathrm{r}(\boldsymbol{A}.\boldsymbol{B}) = \mathrm{r}(\boldsymbol{A})$.
(3) *Hodnost nenulové matice $\boldsymbol{A}$ je rovna největšímu řádu nějaké její regulární submatice.*
(4) $\mathrm{r}(\boldsymbol{A}) = n - \dim \mathcal{N}(\boldsymbol{A})$.
(5) *V případě $\mathbb{F} \subseteq \mathbb{C}$ platí* $\mathrm{r}(\boldsymbol{A}.\boldsymbol{A}^*) = \mathrm{r}(\boldsymbol{A}^*.\boldsymbol{A}) = \mathrm{r}(\boldsymbol{A}) = \mathrm{r}(\boldsymbol{A}^*)$ *a speciálně je-li $\boldsymbol{A}$ sloupcově, resp. řádkově plné hodnosti, pak $\boldsymbol{A}^*.\boldsymbol{A}$, resp. $\boldsymbol{A}.\boldsymbol{A}^*$ je regulární.*
(5') *V případě $\mathbb{F} \subseteq \mathbb{R}$ platí* $\mathrm{r}(\boldsymbol{A}.\boldsymbol{A}^T) = \mathrm{r}(\boldsymbol{A}^T.\boldsymbol{A}) = \mathrm{r}(\boldsymbol{A}) = \mathrm{r}(\boldsymbol{A}^T)$ *a speciálně je-li $\boldsymbol{A}$ sloupcově, resp. řádkově plné hodnosti, pak $\boldsymbol{A}^T.\boldsymbol{A}$, resp. $\boldsymbol{A}.\boldsymbol{A}^T$ je regulární.*

Důkaz.

(1) Hodnost matice odpovídá maximálnímu počtu lineárně nezávislých sloupců (řádků) matice a nemůže proto přesáhnout dimenzi prostoru, do něhož náleží, tj. musí platit $\mathrm{r}(\boldsymbol{A}) \leq m$ a současně $\mathrm{r}(\boldsymbol{A}) \leq n$.
(2) $\mathcal{R}(\boldsymbol{A}.\boldsymbol{B}) \subseteq \mathcal{R}(\boldsymbol{A}) \overset{3.24(3)}{\Rightarrow} \dim \mathcal{R}(\boldsymbol{A}.\boldsymbol{B}) \leq \dim \mathcal{R}(\boldsymbol{A}) \overset{4.17}{\Rightarrow}$ $\Rightarrow \mathrm{r}(\boldsymbol{A}.\boldsymbol{B}) \leq \mathrm{r}(\boldsymbol{A})$. Užitím této nerovnosti na transpozici součinu dostaneme i druhou nerovnost:
$\mathrm{r}(\boldsymbol{A}.\boldsymbol{B}) \overset{4.23}{=} \mathrm{r}((\boldsymbol{A}.\boldsymbol{B})^T) = \mathrm{r}(\boldsymbol{B}^T.\boldsymbol{A}^T) \leq \mathrm{r}(\boldsymbol{B}^T) \overset{4.23}{=} \mathrm{r}(\boldsymbol{B})$.
Je-li $\boldsymbol{B}$ řádkově plné hodnosti, pak $\mathrm{r}(\boldsymbol{A}.\boldsymbol{B}) \overset{4.24(1)}{=} \mathrm{r}(\boldsymbol{A}) = \min(\mathrm{r}(\boldsymbol{A}), \mathrm{r}(\boldsymbol{B}))$, neboť dle (1) je $\mathrm{r}(\boldsymbol{A}) \leq \min(m, n) \leq n = \mathrm{r}(\boldsymbol{B})$. Analogicky pro $\boldsymbol{A}$ sloupcově plné hodnosti:
$\mathrm{r}(\boldsymbol{A}.\boldsymbol{B}) \overset{4.24(1)}{=} \mathrm{r}(\boldsymbol{B}) = \min(\mathrm{r}(\boldsymbol{A}), \mathrm{r}(\boldsymbol{B}))$, neboť dle (1) máme $\mathrm{r}(\boldsymbol{B}) \leq \min(n, p) \leq n = \mathrm{r}(\boldsymbol{A})$.

(3) $\boldsymbol{A}$ nenulová $\Rightarrow$ existuje alespoň jeden nenulový prvek a_{ij} určující regulární submatici $[a_{ij}]$ řádu 1. Označíme-li r největší řád nějaké regulární submatice, pak tedy $r \geq 1$ a dle 4.19(3) lze v matici vybrat r nezávislých řádků (resp. sloupců), které lze doplnit na bázi o $h := \mathrm{r}(\boldsymbol{A})$ prvcích. Platí tedy $h \geq r$. Naopak z matice $\boldsymbol{A}$ hodnosti h lze vybrat submatici $\boldsymbol{B}$ o h lineárně nezávislých sloupcích (sloupcová báze), která má sloupcovou plnou hodnost h. Dle 4.23 je i řádková hodnost matice $\boldsymbol{B}$ rovna h, takže z $\boldsymbol{B}$ lze vybrat h nezávislých řádků. Výsledná submatice řádu h má rovněž h nezávislých řádků (a tedy i sloupců) a je proto regulární. Protože r udává největší řád takové submatice, platí i opačná nerovnost $h \leq r$ a celkem tedy $h = r$. Takto zkonstruovaná submatice má pak největší možný řád h.

(4) Nechť $\boldsymbol{A} = \boldsymbol{B}.\boldsymbol{C}$ je skeletní rozklad podle věty 4.22, $r := \mathrm{r}(\boldsymbol{A})$. Nechť $\boldsymbol{Q}$ je vhodná permutační matice (viz 4.14(11)), kterou přeuspořádáme sloupce $\boldsymbol{C}$ tak, aby jednotková matice $\boldsymbol{I}_r$ obsažená v $\boldsymbol{C}$ byla jejím prvním blokem: $\boldsymbol{C}.\boldsymbol{Q} =: [\boldsymbol{I}_r, \boldsymbol{C}']$. Stejným způsobem přeuspořádáme vektory $\boldsymbol{x} \in \mathbb{F}^n$: $\boldsymbol{Q}^T.\boldsymbol{x} =: [\boldsymbol{y}; \boldsymbol{t}]$, kde výsledný vektor rozdělíme na dva sloupcové bloky $\boldsymbol{y} \in \mathbb{F}^r$ a $\boldsymbol{t} \in \mathbb{F}^{n-r}$. Pak dostáváme:

$$\boldsymbol{x} \in \mathcal{N}(\boldsymbol{A}) \overset{4.22}{=} \mathcal{N}(\boldsymbol{C}) \;\Leftrightarrow\; \boldsymbol{C}.\boldsymbol{x} = \boldsymbol{0} \overset{4.28(3)}{\Leftrightarrow} \boldsymbol{C}.\boldsymbol{Q}.\boldsymbol{Q}^T.\boldsymbol{x} = \boldsymbol{0}$$
$$\Leftrightarrow\; [\boldsymbol{I}_r, \boldsymbol{C}'].[\boldsymbol{y}; \boldsymbol{t}] = \boldsymbol{0} \;\Leftrightarrow\; \boldsymbol{I}_r.\boldsymbol{y} + \boldsymbol{C}'.\boldsymbol{t} = \boldsymbol{0} \;\Leftrightarrow\; \boldsymbol{y} = -\boldsymbol{C}'.\boldsymbol{t}$$
$$\Leftrightarrow\; [\boldsymbol{y}; \boldsymbol{t}] = \underbrace{[-\boldsymbol{C}'; \boldsymbol{I}_{n-r}]}_{=:\boldsymbol{C}''}.\boldsymbol{t} \;\Leftrightarrow\; \boldsymbol{x} = \boldsymbol{Q}.[\boldsymbol{y}; \boldsymbol{t}] \in \mathcal{R}(\boldsymbol{Q}.\boldsymbol{C}'').$$

Tedy $\mathcal{N}(\boldsymbol{A}) = \mathcal{R}(\boldsymbol{Q}.\boldsymbol{C}'') \Rightarrow \dim \mathcal{N}(\boldsymbol{A}) = \dim \mathcal{R}(\boldsymbol{Q}.\boldsymbol{C}'') = \mathrm{r}(\boldsymbol{Q}.\boldsymbol{C}'') \overset{4.24(5)}{=} \mathrm{r}(\boldsymbol{C}'') \overset{(3)}{=} n - r$, neboť $\boldsymbol{C}''$ obsahuje regulární submatici $\boldsymbol{I}_{n-r}$, která je maximálního možného řádu, protože $n - r$ je sloupcový rozměr matice $\boldsymbol{C}''$.

(5) Rovnost hodností plyne z 3.88(5)(iii),(iv). $\boldsymbol{A}$ sloupcově plné hodnosti $\Rightarrow \mathrm{r}(\boldsymbol{A}) = n \Rightarrow \boldsymbol{A}^*.\boldsymbol{A}$ je řádu n o hodnosti n a tedy

regulární. Podobně $\boldsymbol{A}$ řádkově plné hodnosti $\Rightarrow \boldsymbol{A}^*$ má sloupcově plnou hodnost m. Pak dle předchozí části po záměně role $\boldsymbol{A}$ a $\boldsymbol{A}^*$ dostáváme: $\mathrm{r}(\boldsymbol{A}.\boldsymbol{A}^*) = \mathrm{r}(\boldsymbol{A}^{**}.\boldsymbol{A}^*) = \mathrm{r}(\boldsymbol{A}^*) = m$. Matice $\boldsymbol{A}.\boldsymbol{A}^*$ je řádu m a tedy regulární.

(5') Je důsledkem (5), neboť v případě reálné matice je $\boldsymbol{A}^* = \boldsymbol{A}^T$ dle 4.11(5).

$\square$

<u>DŮSLEDEK</u> 4.30. *Hodnost schodovité matice je rovna počtu jejích nenulových řádků (tzv. schodů).*

Důkaz. Pro nulovou matici je tvrzení zřejmé. Nechť $\boldsymbol{S}$ typu m/n je schodovitá matice s k nenulovými řádky, $k \geq 1$. Vynecháme-li $m-k$ nulových řádků, dostaneme dle 4.24(9) matici $\boldsymbol{S}'$ typu k/n stejné hodnosti: $\mathrm{r}(\boldsymbol{S}) = \mathrm{r}(\boldsymbol{S}')$. Podle 4.6 matice $\boldsymbol{S}'$ obsahuje horní trojúhelníkovou submatici řádu k s nenulovou diagonálou, která je regulární dle 4.27. Jelikož řádkový rozměr matice $\boldsymbol{S}'$ je k, je tato submatice maximální taková a tedy celkem $\mathrm{r}(\boldsymbol{S}) = \mathrm{r}(\boldsymbol{S}') \overset{4.29(3)}{=} k$. $\square$

PŘÍKLAD 4.31. Vlastnost (5') neplatí obecně pro matice s prvky z nereálného skalárního pole $\mathbb{F}$. Jednoduchý protipříklad najdeme již v případě komplexních matic ($\mathbb{F} = \mathbb{C}$): Uvažujme matici

$$\boldsymbol{A} = \begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix}, \text{ kde } [-i, 1] = -i[1, i] \Rightarrow \mathrm{r}(\boldsymbol{A}) = 1.$$

Totiž za sloupcovou (řádkovou) bázi (maximální lineárně nezávislou podmnožinu) matice $\boldsymbol{A}$ lze v tomto případě zvolit jednoprvkovou množinu tvořenou libovolným sloupcem (řádkem), neboť každá jednoprvková množina obsahující nenulový vektor je triviálně lineárně nezávislá dle 3.3(L5). Pak dostáváme

$$\boldsymbol{A}.\boldsymbol{A}^T = \begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix} . \begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \Longrightarrow \quad \mathrm{r}(\boldsymbol{A}.\boldsymbol{A}^T) = 0.$$

$$\boldsymbol{A}^T.\boldsymbol{A} = \begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix} . \begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \Longrightarrow \quad \mathrm{r}(\boldsymbol{A}^T.\boldsymbol{A}) = 0.$$

Podstata problému tkví v tom, že prvky například matice $\boldsymbol{A}^T.\boldsymbol{A}$ jsou sice konstruovány podobně jako u Gramovy matice v 4.14(9), tj. jsou ve tvaru výrazů $x_1y_1 + x_2y_2$, kde $\boldsymbol{x}$ a $\boldsymbol{y}$ jsou vybrány ze sloupců $\boldsymbol{A}$. Tyto výrazy jsou skalárními součiny v $\mathbb{R}$, nikoliv avšak v $\mathbb{C}$, kde ztrácíme platnost axiomu (S3) a tím i ortogonalitu: například pro sloupce $\boldsymbol{A}$ máme $\langle[1,-i],[i,1]\rangle = 1.\bar{i} + (-i).\bar{1} = 1.(-i) + (-i).1 = -2.i \neq 0$, i když $1.i + (-i).1 = 0$. Vzhledem k 3.68 tak nemáme garantovánu ani lineární nezávislost, kterou jsme v tomto příkladu skutečně ztratili.
Ztratili jsme takto dokonce i vlastnost ortogonálního rozkladu dle 3.88(5)(i), přestože 3.88(5)(v) platí dle 4.29(4): $\dim \mathcal{N}(A) = \dim \mathbb{C}^2 - \mathrm{r}(A) = 2 - 1 = 1$. Totiž $\mathbb{C}^2$ nemůže být ortogonálním součtem podprostorů $\mathcal{R}(\boldsymbol{A}^T)$ a $\mathcal{N}(\boldsymbol{A})$, neboť není ani jejich přímým součtem: 1. sloupec v $\boldsymbol{A}.\boldsymbol{A}^T$ je roven $\boldsymbol{A}.[1,i]^T = [0,0]^T \Rightarrow [1,i]^T \in \mathcal{N}(\boldsymbol{A})$. Současně ale také $\boldsymbol{A}^T.[1,0]^T = [1,i]^T \Rightarrow [1,i]^T \in \mathcal{R}(\boldsymbol{A}^T)$ a tedy $\boldsymbol{0} \neq [1,0]^T \in \mathcal{R}(\boldsymbol{A}^T) \cap \mathcal{N}(\boldsymbol{A}) \overset{3.43}{\Rightarrow} \mathcal{R}(\boldsymbol{A}^T) + \mathcal{N}(\boldsymbol{A}) \neq \mathcal{R}(\boldsymbol{A}^T) \dot{+} \mathcal{N}(\boldsymbol{A})$.

<u>*POZNÁMKA*</u> 4.32 (Maticový zápis bilineární a kvadratické formy).
Nechť $\boldsymbol{A} =: [a_{ij}]$ je čtvercová matice řádu n a $\boldsymbol{x} =: [x_1; \dots; x_n]$, $\boldsymbol{y} =: [y_1; \dots; y_n]$ vektory z $\mathbb{F}^n$.
Bilineární forma určená maticí $\boldsymbol{A}$ je funkce $\mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}$ definovaná vztahem:

$$\boldsymbol{y}^T.\boldsymbol{A}.\boldsymbol{x} = \sum_{i=1}^{n} (\sum_{j=1}^{n} a_{ij}x_j) y_i = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} y_i x_j,$$

kde výraz v závorce je i-tá složka vektoru $\boldsymbol{A}.\boldsymbol{x}$.
Pro $\boldsymbol{x} = \boldsymbol{y}$ bilineární forma přejde v zobrazení $\mathbb{F}^n \to \mathbb{F}$ a nazývá se

kvadratickou formou určenou maticí $\boldsymbol{A}$:

$$\boldsymbol{x}^T.\boldsymbol{A}.\boldsymbol{x} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_ix_j.$$

V případě $\mathbb{F} \subseteq \mathbb{R}$ je můžeme vzhledem k 4.14(9) a 4.15(6) vyjádřit také pomocí skalárního součinu:
$\boldsymbol{y}^T.\boldsymbol{A}.\boldsymbol{x} = \langle \boldsymbol{A}.\boldsymbol{x}, \boldsymbol{y}\rangle$, resp. $\boldsymbol{x}^T.\boldsymbol{A}.\boldsymbol{x} = \langle \boldsymbol{A}.\boldsymbol{x}, \boldsymbol{x}\rangle$, což je v souladu s poznámkou 3.84. V komplexním případě $\mathbb{F} \subseteq \mathbb{C}$ užijeme $\boldsymbol{A}^*$ místo $\boldsymbol{A}^T$, takže dostáváme vyjádření:

$$\langle \boldsymbol{A}.\boldsymbol{x}, \boldsymbol{y}\rangle = \boldsymbol{y}^*.\boldsymbol{A}.\boldsymbol{x} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}\overline{y}_ix_j,$$

$$\langle \boldsymbol{A}.\boldsymbol{x}, \boldsymbol{x}\rangle = \boldsymbol{x}^*.\boldsymbol{A}.\boldsymbol{x} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}\overline{x}_ix_j.$$

Matice $\boldsymbol{A}$ se nazývá **pozitivně semidefinitní (pozitivně definitní)**, jestliže určuje operátor, který je pozitivní (striktně pozitivní) ve smyslu poznámky 3.84. V takovém případě kvadratická forma nabývá pouze reálných nezáporných hodnot (kladných hodnot pro $\boldsymbol{x} \neq \boldsymbol{0}$) a $\boldsymbol{A}$ je hermitovsky symetrická matice.

4.4. PŘEVOD NA SCHODOVITÝ TVAR A LU-ROZKLAD.

Věta 4.29 sice uvádí některé užitečné vlastnosti hodnosti matic umožňující její zjištění v některých speciálních případech, nikoliv však obecně pro libovolnou zadanou matici $\boldsymbol{A}$, řekněme typu m/n. V tomto odstavci odvodíme univerzální algoritmus tzv. **Gaussovy eliminace**, který požadovanou úlohu beze zbytku řeší a navíc dává konstrukci báze obou prostorů svázaných s maticí (operátorem) $\boldsymbol{A}$, tj. jak oboru hodnot $\mathcal{R}(\boldsymbol{A})$, tak jádra $\mathcal{N}(\boldsymbol{A})$. Jako jeho důsledek obdržíme navíc tzv. LU**-rozklad matice** $\boldsymbol{A}$, který představuje jeden z mnoha možných skeletních rozkladů. Na rozdíl od důkazu věty 4.22, který byl nekonstruktivní, Gaussova eliminace poskytuje (nikoliv obecně jednoznačnou) konstrukci takového rozkladu.
Princip Gaussovy eliminace spočívá v postupném provádění elementárních řádkových úprav[16], které nemění hodnost matice. V zásadě vystačíme pouze s úpravami typu (5) a (8) z věty 4.24 a to dokonce ve zjednodušené podobě: záměna dvou řádků a přičtení skalárního násobku nějakého řádku k jinému řádku. V dalším zkonstruujeme speciální regulární transformační matice, kterými budeme danou matici postupně násobit zleva — viz též 4.24(3). Výsledkem bude převod zadané matice $\boldsymbol{A}$ na schodovitý tvar, jehož hodnost (shodná s $\mathrm{r}(\boldsymbol{A})$) se snadno zjistí podle 4.30.

<u>**DEFINICE**</u> **4.33** (Transformační matice pro některé řádkové úpravy)**.**
Nechť m je řádkový rozměr transformované matice $\boldsymbol{A}$.
(1) <u>Záměna i-ho a j-ho řádku</u>:
Nechť $\sigma := \sigma_{ij}$ značí permutaci provádějící záměnu indexu i a j. Pak zřejmě $\sigma = \sigma^{-1}$. Označíme-li $\boldsymbol{P}_{i,j} := \boldsymbol{P}_\sigma$ odpovídající permutační matici řádu m, pak $\boldsymbol{P}_{i,j} = \boldsymbol{P}_{i,j}^{-1} \overset{4.28(3)}{=} \boldsymbol{P}_{i,j}^T$ a tedy při násobení touto maticí zleva (zprava) dochází k záměně i-tého a j-tého řádku (sloupce) — viz 4.14(11). V případě $i = j$ je $\boldsymbol{P}_{ii} = \boldsymbol{I}_m$ identita.

[16] Obdobně je možno provádět sloupcové úpravy. Jelikož je lze transpozicí matice vždy převést na řádkové úpravy, upřednostňujeme nadále tento případ.

(2) Přičtení α-násobku j-ho řádku k i-tému ($i \neq j$):

Nechť pro $\alpha \in \mathbb{F}$ značí $\boldsymbol{R}_{ij}^{(\alpha)} := \boldsymbol{I}_m + \alpha E_{ij}$ čtvercovou matici řádu m. Tato matice je trojúhelníková s jednotkovou diagonálou, prvkem α v i-tém řádku a j-tém sloupci a nulami všude jinde. Zřejmě platí $\boldsymbol{R}_{ij}^{(\alpha)T} = \boldsymbol{R}_{ji}^{(\alpha)}$, přičemž při násobení maticí $\boldsymbol{R}_{ij}^{(\alpha)}$ zleva (maticí $\boldsymbol{R}_{ji}^{(\alpha)}$ zprava) dochází k přičtení α-násobku j-tého řádku (sloupce) k i-tému řádku (sloupci).

(3) Vynásobení i-ho řádku skalárem $\alpha \neq 0$:

Podle 4.14(10) je příslušnou transformační maticí diagonální matice $\boldsymbol{D}_i^{(\alpha)} := \operatorname{diag}(1, \ldots, 1, \alpha, 1, \ldots, 1)$, kde α je i-tým prvkem na jinak jednotkové diagonále.

Věta 4.34 (Vlastnosti transformačních matic $\boldsymbol{P}_{ij}$, $\boldsymbol{R}_{ij}^{(\alpha)}$ a $\boldsymbol{D}_i^{(\alpha)}$**).**
Všechny uvedené matice jsou regulární a platí pro ně:

(1) *Nechť index j je pevný a $\alpha_i \in \mathbb{F}$ je m skalárů ($i = 1, \ldots, m$), kde $\alpha_j = 0$. Pak $\boldsymbol{R}_j^{(\boldsymbol{\alpha})} := \boldsymbol{R}_{1j}^{(\alpha_1)} \ldots \boldsymbol{R}_{mj}^{(\alpha_m)}$ je jednotková matice, k jejímuž j-tému sloupci je přičten vektor $\boldsymbol{\alpha} := [\alpha_1, \ldots, \alpha_m]^T$. Tato matice realizuje složení m řádkových úprav: k i-tému řádku je přičten α_i-násobek j-tého řádku pro $i = 1, ..., m$. Na pořadí provádění těchto úprav (tj. na pořadí násobení matic $\boldsymbol{R}_{ij}^{(\alpha_i)}$) přitom nezáleží. Zřejmě $\boldsymbol{\alpha} = \boldsymbol{0} \Rightarrow \boldsymbol{R}_j^{(\boldsymbol{\alpha})} = \boldsymbol{I}_m$.*

(2) *Výsledná matice $\boldsymbol{R}_j^{(\boldsymbol{\alpha})}$ je regulární a pokud $\alpha_i = 0$ pro $i \leq j$ ($i \geq j$), pak je navíc dolní (horní) trojúhelníková. V takovém případě budeme obvykle psát $\boldsymbol{L}_j^{(\boldsymbol{\alpha})}$ ($\boldsymbol{U}_j^{(\boldsymbol{\alpha})}$) místo[17] $\boldsymbol{R}_j^{(\boldsymbol{\alpha})}$. Inverzní matice je určena vztahem: $(\boldsymbol{R}_j^{(\boldsymbol{\alpha})})^{-1} = \boldsymbol{R}_j^{(-\boldsymbol{\alpha})}$. Je tedy téhož typu, kde pouze skaláry mají obrácené znaménko. Zejména také dostáváme $(\boldsymbol{R}_{ij}^{(\alpha)})^{-1} = \boldsymbol{R}_{ij}^{(-\alpha)}$, neboť $\boldsymbol{R}_{ij}^{(\alpha)}$ je speciálním případem matice $\boldsymbol{R}_j^{(\boldsymbol{\alpha})}$, kde $\alpha_i = \alpha$ a $\alpha_k = 0$ pro $k \neq i$.*

---

[17] Značení je dáno zvyklostmi anglosaské odborné literatury: písmeno $\boldsymbol{L}$, resp. $\boldsymbol{U}$ je odvozeno od počátečních písmen slov *Lower* a *Upper*.

(3) *Pro libovolné tři indexy* $i, j, k \in \{1, \dots, m\}$, $i \neq j$, $k \neq j$ *platí* $\boldsymbol{P}_{ik}.\boldsymbol{R}_j^{(\boldsymbol{\alpha})} = \boldsymbol{R}_j^{(\boldsymbol{P}_{ik}.\boldsymbol{\alpha})}.\boldsymbol{P}_{ik}$.

Tedy matice $\boldsymbol{P}_{ik}$ *a* $\boldsymbol{R}_j^{(\boldsymbol{\alpha})}$ *jsou při násobení záměnitelné až na pořadí skalárů ve vektoru* $\boldsymbol{\alpha}$, *kde dojde k záměně jeho složek* α_i *a* α_k.

(4) $\boldsymbol{L} := \boldsymbol{L}_1^{(\boldsymbol{\alpha}_1)}.\boldsymbol{L}_2^{(\boldsymbol{\alpha}_2)} \dots \boldsymbol{L}_m^{(\boldsymbol{\alpha}_m)}$ *a* $\boldsymbol{U} := \boldsymbol{U}_m^{(\boldsymbol{\alpha}_m)}.\boldsymbol{U}_{m-1}^{(\boldsymbol{\alpha}_{m-1})} \dots \boldsymbol{U}_1^{(\boldsymbol{\alpha}_1)}$ *je po řadě regulární dolní a horní trojúhelníková matice s jednotkovou diagonálou, kde* $L(i,j) = \alpha_j(i)$ *a* $U(i,j) = \alpha_j(i)$ *pro každé* $i \neq j$, *neboli sloupce v* $\boldsymbol{L}$, *resp.* $\boldsymbol{U}$ *odpovídají po řadě příslušným sloupcům matic* $\boldsymbol{L}_j^{(\boldsymbol{\alpha}_j)}$, *resp.* $\boldsymbol{U}_j^{(\boldsymbol{\alpha}_j)}$. *Poznamenejme, že na rozdíl od (1) v tomto případě již záleží na pořadí provádění úprav (tj. na pořadí násobení matic* $\boldsymbol{L}_j^{(\boldsymbol{\alpha}_j)}$, *resp.* $\boldsymbol{U}_j^{(\boldsymbol{\alpha}_j)}$*).*

(5) $\boldsymbol{D}_1^{(\alpha_1)}.\boldsymbol{D}_2^{(\alpha_2)} \dots \boldsymbol{D}_m^{(\alpha_m)} = \operatorname{diag}(\alpha_1, \alpha_2, \dots, \alpha_m)$ *je při všech nenulových* $\alpha_i \neq 0$ *regulární diagonální matice. Tato matice realizuje složení m řádkových úprav: i-tý řádek je vynásoben skalárem* α_i *pro* $i = 1, ..., m$. *Na pořadí provádění těchto úprav (tj. na pořadí násobení matic* $\boldsymbol{D}_i^{(\alpha_i)}$*) přitom nezáleží.*

Důkaz. Pro větší názornost zobrazme nejprve strukturu matice $\boldsymbol{R}_j^{(\boldsymbol{\alpha})}$:

$$\boldsymbol{R}_j^{(\boldsymbol{\alpha})} = \begin{bmatrix} 1 & \dots & 0 & \alpha_1 & 0 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & \alpha_{j-1} & 0 & \dots & 0 & \dots & 0 \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 & \dots & 0 \\ 0 & \dots & 0 & \alpha_{j+1} & 1 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \alpha_i & 0 & \dots & 1 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \alpha_m & 0 & \dots & 0 & \dots & 1 \end{bmatrix}.$$

Všechny uvažované matice jsou buď trojúhelníkové nebo diagonální s jednotkovou diagonálou, případně jsou součinem takových matic. Podle 4.27 a případně i s ohledem na 4.24(4) jsou tedy regulární. Součin dolních (horních) trojúhelníkových matic je opět matice téhož typu dle 4.14(12). Strukturu matic ve tvaru součinu si čtenář snadno odvodí jako snadné cvičení provedením tohoto součinu, resp. příslušných řádkových úprav při postupném násobení zprava doleva. Při důkazu tvrzení (2) stačí podobně na základě věty 4.25 ověřit přímým vynásobením platnost identit: $\boldsymbol{R}_j^{(-\boldsymbol{\alpha})}.\boldsymbol{R}_j^{(\boldsymbol{\alpha})} = \boldsymbol{R}_j^{(\boldsymbol{\alpha})}.\boldsymbol{R}_j^{(-\boldsymbol{\alpha})} = \boldsymbol{I}_m$. □

Poznámka 4.35.
Je-li $\boldsymbol{A}$ matice typu m/n, pak s uvážením 4.14(8)b) snadno nahlédneme, že $\boldsymbol{R}_j^{(\boldsymbol{\alpha})}.\boldsymbol{A} = \boldsymbol{A}+\boldsymbol{\alpha}.A(j,:)$. Maticový výraz vpravo tak představuje alternativní způsob provedení stejných řádkových úprav v matici $\boldsymbol{A}$, jaké odpovídají násobení maticí $\boldsymbol{R}_j^{(\boldsymbol{\alpha})}$ zleva. V některých situacích může být tento druhý způsob z hlediska programové implementace efektivnější, neboť není třeba dopředu vytvářet a do paměti ukládat matici $\boldsymbol{R}_j^{(\boldsymbol{\alpha})}$, která je **řídká** (má velké množství nulových prvků), což může vést k plýtvání pamětí.

VĚTA 4.36 (Převod matice na schodovitý tvar Gaussovou eliminací[18]). *Každá matice se dá konečným počtem řádkových elementárních transformací typu 4.33(1),(2) převést na matici ve schodovitém tvaru o stejné hodnosti.*

DŮKAZ. Důkaz této věty je konstruktivní, to znamená, že dává postup řešení této úlohy, který je možno použít v konkrétním případě. Tento postup bývá nazýván *Gaussův algoritmus* a spočívá v následujících krocích pro matici $\boldsymbol{A} =: [a_{ij}]$ typu m/n:

(G0) Jestliže matice $\boldsymbol{A}$ je nulová, již je ve schodovitém tvaru a jsme hotovi.

(G1) V opačném případě nechť j_1 je index prvního nenulového sloupce. Existuje tedy $k \in \mathbb{N}$, $1 \le k \le m$ tak, že $a_{kj_1} \neq 0$.

[18] viz též skripta `[KaSk:V9.3 s.80-81]` nebo `[Šik:V1.26 s.9-10]`

Řádek k-tý vyměňme s prvním řádkem, pokud $k \neq 1$. Tím dostaneme matici $\boldsymbol{B} =: [b_{uv}]$ typu m/n takovou, že sloupce $1, 2, \dots, j_1 - 1$ jsou nulové a $b_{1j_1} \neq 0$.

(G2) V matici B ke každému u-tému řádku ($2 \leq u \leq m$) přičteme první řádek vynásobený číslem $-\frac{b_{uj_1}}{b_{1j_1}}$. Dostaneme matici $\boldsymbol{C} = [c_{uv}]$ typu m/n takovou, že sloupce $1, 2, \dots, j_1 - 1$ jsou nulové, $c_{1j_1} \neq 0$ a $c_{uj_1} = 0$ pro každé $2 \leq u \leq m$.

Tím je určen první řádek hledané schodovité matice. Není-li matice $\boldsymbol{C}$ ještě ve schodovitém tvaru, aplikujeme kroky (G1) a (G2) na submatici $C([2, \dots, m], :)$. Po jejich provedení bude druhý řádek celé matice druhým řádkem hledané schodovité matice, atd. Tímto způsobem postupujeme tak dlouho, až obdržíme matici ve schodovitém tvaru, tj. jakmile buď byl proveden maximální možný počet kroků m a nebo všechny zbývající řádky jsou již nulové. $\square$

Důsledek 4.37 (Maticový zápis Gaussovy eliminace)**.**
Nechť $\boldsymbol{A}$ je matice typu m/n, $\mathrm{r}(\boldsymbol{A}) = r$. Pak Gaussova eliminace rekurentně konstruuje posloupnost matic $\boldsymbol{A} =: \boldsymbol{A}_0 \sim \boldsymbol{A}_1 \sim \cdots \sim \boldsymbol{A}_r =: \boldsymbol{S}$ téže hodnosti, kde $\boldsymbol{S} =: [s_{ij}]$ je schodovitá matice s r nenulovými řádky (schody) a horní trojúhelníkovou submaticí řádu r s diagonálovými prvky $s_{ij_i} \neq 0$, $1 \leq j_1 < \cdots < j_r \leq n$ (viz 4.6). Nechť pro $i \in \{1, \dots, r\}$ byla již zkonstruována matice $\boldsymbol{A}_{i-1}$. Pak $\boldsymbol{A}_i$ dostaneme ve dvou krocích takto:

(G1) *<u>Záměna i-tého a k-ho řádku v matici $\boldsymbol{A}_{i-1}$:</u>*
$\boldsymbol{B}_i := \boldsymbol{P}_i.\boldsymbol{A}_{i-1} =: [b_{uv}]$, *kde* $\boldsymbol{P}_i := \boldsymbol{P}_{ik}$ *pro vhodné* $i \leq k \leq m$ *takové, že* $A_{i-1}(k, j_i) \neq 0$ *(k závisí na i). Takto zajistíme* $b_{ij_i} \neq 0$.

(G2) *<u>Eliminace koncové části j_i-tého sloupce v matici $\boldsymbol{B}_i$:</u>*
$\boldsymbol{A}_i := \boldsymbol{L}_i^{(\boldsymbol{\beta}_i)}.\boldsymbol{B}_i$, *kde* $\boldsymbol{\beta}_i = [\underbrace{0, \dots, 0}_{i\times}, -\frac{b_{i+1j_i}}{b_{ij_i}}, \dots, -\frac{b_{mj_i}}{b_{ij_i}}]^T$.

Sloučením obou kroků do jednoho dostáváme rekurentní vztah:
$\boldsymbol{A}_i = \boldsymbol{L}_i^{(\boldsymbol{\beta}_i)}.\boldsymbol{P}_i.\boldsymbol{A}_{i-1}$ *pro* $i = 1, \dots, r$.

Sloučením všech kroků, pak dostáváme:
$\boldsymbol{R}.\boldsymbol{A} = \boldsymbol{S}$, *kde* $\boldsymbol{R} := \boldsymbol{L}_r^{(\boldsymbol{\beta}_r)}.\boldsymbol{P}_r \dots \boldsymbol{L}_2^{(\boldsymbol{\beta}_2)}.\boldsymbol{P}_2.\boldsymbol{L}_1^{(\boldsymbol{\beta}_1)}.\boldsymbol{P}_1$ *je regulární matice řádu* m *realizující provedení všech elementárních úprav převodu na schodovitý tvar.*

Důkaz. Transformační vztahy jsou důsledkem 4.33(1) a 4.34(1)(2), kde transformační matice $\boldsymbol{R}_i^{(\boldsymbol{\beta}_i)} = \boldsymbol{L}_i^{(\boldsymbol{\beta}_i)}$ je skutečně dolní trojúhelníková, neboť $\beta_i(u) = 0$ pro $u \leq i$. Volba $\beta_i(u) = -\frac{b_{uj_i}}{b_{ij_i}}$ pro $i+1 \leq u \leq m$ pak zajistí požadovanou eliminaci koncové části j_i-tého sloupce, neboť přičtením $\beta_i(j)$-tého násobku i-tého řádku matice $\boldsymbol{B}_i$ k jejímu u-tému řádku dostáváme:
a) $\underline{j_i\text{-tý sloupec:}}$
$A_i(u, j_i) = b_{uj_i} + \beta_i(u) b_{ij_i} = b_{uj_i} + (-\frac{b_{uj_i}}{b_{ij_i}}) b_{ij_i} = 0.$
b) $\underline{\text{Úvodní sloupce pro } 1 \leq v < j_i:}$
$A_i(u, v) = b_{uv} + \beta_i(u) b_{iv} = 0$ zůstávají nulové, neboť $b_{uv} = b_{iv} = 0$ byly nulové již z předchozích kroků.

Regularita výsledné transformační matice $\boldsymbol{R}$ je důsledkem 4.24(4) a regularity všech zúčastněných matic. □

<u>DŮSLEDEK</u> 4.38 (LU-rozklad matice)**.**
Platí $\boldsymbol{L}.\boldsymbol{S} = \boldsymbol{P}.\boldsymbol{A}$, *kde* $\boldsymbol{L} =: [l_{ui}]$ *je čtvercová dolní trojúhelníková matice řádu* m *s jednotkovou diagonálou (*$l_{ii} = 1$ *pro* $i = 1, \dots, m$*) a pod hlavní diagonálou s prvky* $l_{ui} = \begin{cases} \frac{b'_{uj_i}}{b'_{ij_i}} & \text{pro } i = 1, \dots, r \\ 0 & \text{pro } i = r+1, \dots, m \end{cases}$, *kde* $u = i+1, \dots, m$ *a* b'_{uj_i} *jsou prvky z* j_i*-tého sloupce matice* $\boldsymbol{B}'_i := \boldsymbol{A}_{i-1}$ *ze všech* r *kroků (G1) provedených během Gaussovy eliminace předem permutované matice* $\boldsymbol{P}.\boldsymbol{A}$, *přičemž* $\boldsymbol{P} = \boldsymbol{P}_r \dots \boldsymbol{P}_2.\boldsymbol{P}_1$ *je matice permutace vzniklé složením všech* r *řádkových záměn provedených v krocích (G1) během Gaussovy eliminace původní nepermutované matice* $\boldsymbol{A}$.

• *Označíme-li* $\boldsymbol{L}' := L(:, [1, \ldots, r])$ *a* $\boldsymbol{S}' = S([1, \ldots, r], :)$ *submatice po řadě v* $\boldsymbol{L}$*, resp.* $\boldsymbol{S}$ *tvořené jejich prvými* r *sloupci, resp. řádky, dostáváme modifikovaný rozklad* $\boldsymbol{L}'.\boldsymbol{S}' = \boldsymbol{P}.\boldsymbol{A}$.
• *Je-li speciálně* $\boldsymbol{A}$ *čtvercová a regulární, pak* $\boldsymbol{L}' = \boldsymbol{L}$ *a* $\boldsymbol{S}' = \boldsymbol{S} =: \boldsymbol{U}$*, kde* $\boldsymbol{U}$ *je horní trojúhelníková matice s nenulovou diagonálou, takže dostáváme rozklad* $\boldsymbol{L}.\boldsymbol{U} = \boldsymbol{P}.\boldsymbol{A}$*, který je obvykle nazýván* **LU-rozkladem matice** $\boldsymbol{A}$*. V dalším takto budeme nazývat i kterýkoli z výše uvedených obecnějších rozkladů* $\boldsymbol{L}.\boldsymbol{S} = \boldsymbol{P}.\boldsymbol{A}$ *nebo* $\boldsymbol{L}'.\boldsymbol{S}' = \boldsymbol{P}.\boldsymbol{A}$*, které jsou platné pro libovolnou matici* $\boldsymbol{A}$.

Důkaz.
Matice $\boldsymbol{L}$ má tuto strukturu:

$$\boldsymbol{L} = \begin{bmatrix} 1 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \frac{b'_{2j_1}}{b'_{1j_1}} & 1 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \frac{b'_{rj_1}}{b'_{1j_1}} & \frac{b'_{rj_2}}{b'_{2j_2}} & \ldots & 1 & 0 & \ldots & 0 \\ \frac{b'_{r+1j_1}}{b'_{1j_1}} & \frac{b'_{r+1j_2}}{b'_{2j_2}} & \ldots & \frac{b'_{r+1j_r}}{b'_{rj_r}} & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \frac{b'_{mj_1}}{b'_{1j_1}} & \frac{b'_{mj_2}}{b'_{2j_2}} & \ldots & \frac{b'_{mj_r}}{b'_{rj_r}} & 0 & \ldots & 1 \end{bmatrix}.$$

• Konstrukce rozkladu $\boldsymbol{L}.\boldsymbol{S} = \boldsymbol{P}.\boldsymbol{A}$:
Dle 4.37 platí $\boldsymbol{S} = \boldsymbol{R}.\boldsymbol{A}$, kde $\boldsymbol{R} := \boldsymbol{L}_r^{(\boldsymbol{\beta}_r)}.\boldsymbol{P}_r \ldots \boldsymbol{L}_2^{(\boldsymbol{\beta}_2)}.\boldsymbol{P}_2.\boldsymbol{L}_1^{(\boldsymbol{\beta}_1)}.\boldsymbol{P}_1$.
Užijme opakovaně 4.34(3) pro postupné provádění záměn:
$\boldsymbol{P}_2.\boldsymbol{L}_1^{(\boldsymbol{\beta}_1)} = \boldsymbol{L}_1^{(\boldsymbol{P}_2.\boldsymbol{\beta}_1)}.\boldsymbol{P}_2$,
$\boldsymbol{P}_3.\boldsymbol{L}_2^{(\boldsymbol{\beta}_2)} = \boldsymbol{L}_2^{(\boldsymbol{P}_3.\boldsymbol{\beta}_2)}.\boldsymbol{P}_3$, $\boldsymbol{P}_3.\boldsymbol{L}_1^{(\boldsymbol{P}_2.\boldsymbol{\beta}_1)} = \boldsymbol{L}_1^{(\boldsymbol{P}_3.\boldsymbol{P}_2.\boldsymbol{\beta}_1)}.\boldsymbol{P}_3$, atd.
Po jejich provedení obdržíme:
$\boldsymbol{S} = \boldsymbol{L}_r^{(\boldsymbol{\beta}_r)}.\boldsymbol{L}_{r-1}^{(\boldsymbol{P}_r.\boldsymbol{\beta}_{r-1})} \ldots \boldsymbol{L}_2^{(\boldsymbol{P}_r \ldots \boldsymbol{P}_3.\boldsymbol{\beta}_2)}.\boldsymbol{L}_1^{(\boldsymbol{P}_r \ldots \boldsymbol{P}_2.\boldsymbol{\beta}_1)}.\underbrace{\boldsymbol{P}_r \ldots \boldsymbol{P}_1}_{\boldsymbol{P}}.\boldsymbol{A}$.
Odtud:
$\left(\boldsymbol{L}_r^{(\boldsymbol{\beta}_r)}.\boldsymbol{L}_{r-1}^{(\boldsymbol{P}_r.\boldsymbol{\beta}_{r-1})} \ldots \boldsymbol{L}_2^{(\boldsymbol{P}_r \ldots \boldsymbol{P}_3.\boldsymbol{\beta}_2)}.\boldsymbol{L}_1^{(\boldsymbol{P}_r \ldots \boldsymbol{P}_2.\boldsymbol{\beta}_1)}\right)^{-1}.\boldsymbol{S} = \boldsymbol{P}.\boldsymbol{A}$.

Stačí jen upravit inverzi ze součinu matic vlevo, kterou označíme $\boldsymbol{L}$:
$\boldsymbol{L} := \left(\boldsymbol{L}_r^{(\boldsymbol{\beta}_r)}.\boldsymbol{L}_{r-1}^{(\boldsymbol{P}_r.\boldsymbol{\beta}_{r-1})}\dots\boldsymbol{L}_2^{(\boldsymbol{P}_r\dots\boldsymbol{P}_3.\boldsymbol{\beta}_2)}.\boldsymbol{L}_1^{(\boldsymbol{P}_r\dots\boldsymbol{P}_2.\boldsymbol{\beta}_1)}\right)^{-1} \overset{4.28(2)}{=}$
$\left(\boldsymbol{L}_1^{(\boldsymbol{P}_r\dots\boldsymbol{P}_2.\boldsymbol{\beta}_1)}\right)^{-1}.\left(\boldsymbol{L}_2^{(\boldsymbol{P}_r\dots\boldsymbol{P}_3.\boldsymbol{\beta}_2)}\right)^{-1}\dots\left(\boldsymbol{L}_{r-1}^{(\boldsymbol{P}_r.\boldsymbol{\beta}_{r-1})}\right)^{-1}.\left(\boldsymbol{L}_r^{(\boldsymbol{\beta}_r)}\right)^{-1} \overset{4.34(2)}{=}$
$\boldsymbol{L}_1^{(-\boldsymbol{P}_r\dots\boldsymbol{P}_2.\boldsymbol{\beta}_1)}.\boldsymbol{L}_2^{(-\boldsymbol{P}_r\dots\boldsymbol{P}_3.\boldsymbol{\beta}_2)}\dots\boldsymbol{L}_{r-1}^{(-\boldsymbol{P}_r.\boldsymbol{\beta}_{r-1})}.\boldsymbol{L}_r^{(-\boldsymbol{\beta}_r)}.\underbrace{\boldsymbol{L}_{r+1}^{(\boldsymbol{0})}\dots\boldsymbol{L}_m^{(\boldsymbol{0})}}_{=\boldsymbol{I}_m}.$

Matice $\boldsymbol{L}$ má dle 4.34(4) požadovanou strukturu. K tomu stačí jen uvážit, že permutace $\boldsymbol{P}_r\dots\boldsymbol{P}_{i+1}$ prováděné s vektory koeficientů $\boldsymbol{\beta}_i$ z úpravy matice $\boldsymbol{A}$ přesně odpovídají nepermutovaným vektorům $\boldsymbol{\beta}_i'$ koeficientů z úpravy předem permutované matice $\boldsymbol{P}.\boldsymbol{A}$, kdy krok (G1) vynecháváme, neboť pro každé $i = 1,\dots,r$ již máme předem zajištěno $A_{i-1}(i, j_i) \neq 0$, tj. $\boldsymbol{P}_i = \boldsymbol{I}_m$ a tedy $\boldsymbol{B}_i' := \boldsymbol{A}_{i-1}$ pro každé $i = 1,\dots,m$.

• <u>$\boldsymbol{L}'.\boldsymbol{S}' = \boldsymbol{L}.\boldsymbol{S}$</u>:
Stačí uvážit, že posledních $m-r$ řádků schodovité matice $\boldsymbol{S}$ je nulových, takže při násobení maticí $\boldsymbol{L}$ zleva na jejích hodnotách v posledních $m-r$ sloupcích nezáleží (jsou během součinu násobeny nulami).

• <u>Případ regulární čtvercové matice $\boldsymbol{A}$</u>:
V tomto případě $m = r$, takže $\boldsymbol{L} = \boldsymbol{L}'$ a $\boldsymbol{S} = \boldsymbol{S}'$. Navíc také $n = r$, takže $\boldsymbol{S}$ je čtvercová řádu r a dle 4.6 současně obsahuje regulární horní trojúhelníkovou submatici $\boldsymbol{U}$ téhož řádu r. To může nastat, jen když $\boldsymbol{S} = \boldsymbol{U}$. □

<u>DŮSLEDEK</u> 4.39 (Konstrukce báze prostoru $\mathcal{R}(\boldsymbol{A})$).
Nechť $\boldsymbol{A}$ je matice typu m/n a $\boldsymbol{A} = \boldsymbol{L}.\boldsymbol{S} = \boldsymbol{L}'.\boldsymbol{S}'$ je její LU-rozklad, kde $\boldsymbol{U} = S'(:,[j_1,\dots,j_r])$ je regulární horní trojúhelníková submatice v $\boldsymbol{S}'$. Pak sloupce matice $\boldsymbol{L}'$ tvoří bázi prostoru $\mathcal{R}(\boldsymbol{A})$ a rovněž $A(:,j_1),\dots,A(:,j_r)$ tvoří jeho sloupcovou bázi.

<u>DŮKAZ</u>.
Sloupce $\boldsymbol{L}'$ jsou lineárně nezávislé, neboť jsou vybrány z nezávislé množiny sloupců regulární matice $\boldsymbol{L}$, tvoří tak bázi v $\mathcal{R}(\boldsymbol{L}')$ a současně $\boldsymbol{L}'$ je sloupcově plné hodnosti. Dále
$A(:,[j_1,\dots,j_r]) = \boldsymbol{L}'.S'(:,[j_1,\dots,j_r]) = \boldsymbol{L}'.\boldsymbol{U} \overset{4.24(1)}{\Rightarrow}$

$\mathrm{r}(A(:,[j_1,\ldots,j_r])) = \mathrm{r}(\boldsymbol{S}) = r \overset{4.36}{=} \mathrm{r}(\boldsymbol{A}) \Rightarrow$ sloupce $A(:,j_1),\ldots,A(:,j_r)$ jsou lineárně nezávislé a tvoří proto podle 3.24(4)(ii) bázi prostoru $\mathcal{R}(\boldsymbol{A})$, neboť $\dim \mathcal{R}(\boldsymbol{A}) = r$.
Z vyjádření $\boldsymbol{A} = \boldsymbol{L}'.\boldsymbol{S}'$ současně plyne (viz 4.13a)), že každý sloupec matice $\boldsymbol{A}$ (tj. každý z generátorů prostoru $\mathcal{R}(\boldsymbol{A})$) je lineární kombinací sloupců $\boldsymbol{L}'$, tj. patří do $\mathcal{R}(\boldsymbol{L}')$. Pak $A(:,j_1),\ldots,A(:,j_r)$ musí také tvořit bázi v $\mathcal{R}(\boldsymbol{L}')$ a oba prostory jsou proto stejné. $\square$

<u>DŮSLEDEK</u> 4.40 (Konstrukce báze prostoru $\mathcal{N}(\boldsymbol{A})$)**.**
Nechť $\boldsymbol{A}$ je matice typu m/n a $\boldsymbol{A} = \boldsymbol{L}'.\boldsymbol{S}'$ je její LU-rozklad, kde $\boldsymbol{U} = S'(:,[j_1,\ldots,j_r])$ je regulární horní trojúhelníková submatice v $\boldsymbol{S}'$. Nechť $\boldsymbol{S}''$ je submatice v $\boldsymbol{S}'$ tvořená zbývajícími $n-r$ sloupci nezařazenými do matice $\boldsymbol{U}$. Buď $\boldsymbol{Q}$ vhodná permutační matice, kterou přeuspořádáme sloupce $\boldsymbol{S}''$ tak, aby $\boldsymbol{U}$ byla prvním blokem a $\boldsymbol{S}''$ druhým blokem: $\boldsymbol{S}'.\boldsymbol{Q} = [\boldsymbol{U},\boldsymbol{S}'']$. Pak $n-r$ sloupců blokově sestavené matice $\boldsymbol{N} =: \boldsymbol{Q}.[-\boldsymbol{U}^{-1}.\boldsymbol{S}'';\boldsymbol{I}_{n-r}] \in \mathcal{M}_{n,n-r}$ tvoří bázi prostoru $\mathcal{N}(\boldsymbol{A})$.

<u>DŮKAZ</u>. Všech $n-r$ sloupců matice $\boldsymbol{N}$ je zřejmě lineárně nezávislých, neboť $\boldsymbol{N}$ obsahuje regulární submatici maximálního možného řádu $n-r$ (viz 4.29(3)). Podle téže věty $\dim \mathcal{N}(\boldsymbol{A}) \overset{4.29(4)}{=} n-r$, takže stačí ukázat, že každý sloupec matice $\boldsymbol{N}$ patří do $\mathcal{N}(\boldsymbol{A})$. Podle 4.15(1) je tedy třeba ověřit, že $\boldsymbol{A}.\boldsymbol{N}$ je nulová matice:
$\boldsymbol{A}.\boldsymbol{N} = \boldsymbol{L}'.\boldsymbol{S}'\boldsymbol{Q}.\boldsymbol{Q}^T.\boldsymbol{N} = \boldsymbol{L}'.[\boldsymbol{U},\boldsymbol{S}''].\boldsymbol{Q}^T.\boldsymbol{Q}.[-\boldsymbol{U}^{-1}.\boldsymbol{S}'';\boldsymbol{I}_{n-r}] =$
$\boldsymbol{L}'.[\boldsymbol{U},\boldsymbol{S}''].[-\boldsymbol{U}^{-1}.\boldsymbol{S}'';\boldsymbol{I}_{n-r}] = \boldsymbol{L}'.(-\boldsymbol{U}.\boldsymbol{U}^{-1}.\boldsymbol{S}'' + \boldsymbol{S}''.\boldsymbol{I}_{n-r}) =$
$\boldsymbol{L}'.(-\boldsymbol{S}'' + \boldsymbol{S}'') = \boldsymbol{0}_{n,n-r}$. $\square$

<u>Poznámka</u> 4.41.

(1) Při konstrukci báze prostoru $\mathcal{N}(\boldsymbol{A})$ dle 4.40 se inverzní matice $\boldsymbol{U}^{-1}$ snadno spočte postupem naznačeným v důkazu 4.28(4). V rovnici $\boldsymbol{I}_r = \boldsymbol{X}.\boldsymbol{U}$ postupně počítáme neznámé prvky matice $\boldsymbol{X} := \boldsymbol{U}^{-1}$ srovnáváním prvého sloupce vlevo a vpravo (tím spočteme prvý sloupec $\boldsymbol{X}$), pak prvého řádku vlevo a vpravo (tím dopočteme prvý řádek $\boldsymbol{X}$), pak podobně pro druhý sloupec a řádek, atd. Alternativně můžeme také

řešit maticovou rovnici $\boldsymbol{U}.\boldsymbol{X} = -\boldsymbol{S}''$ postupně pro jednotlivé sloupce: $\boldsymbol{U}.X(:,j) = -S''(:,j)$, což je vzhledem k trojúhelníkové struktuře matice $\boldsymbol{U}$ snadné (podrobněji bude probráno později v odstavci věnovaném řešení systémům lineárních rovnic). Obdržíme tak matici $\boldsymbol{X} = -\boldsymbol{U}^{-1}.\boldsymbol{S}''$, což je právě horní blok ve vyjádření řádkově permutované matice $\boldsymbol{N}$.

(2) LU-rozklad $\boldsymbol{A} = \boldsymbol{L}'.\boldsymbol{S}'$ není nic jiného než speciální případ skeletního rozkladu 4.22, kde $\boldsymbol{L}'$ hraje roli matice $\boldsymbol{B}$ a $\boldsymbol{S}'$ hraje roli matice $\boldsymbol{C}$. Porovnání obou rozkladů ukazuje, že se liší ve dvou aspektech:

- Roli regulární jednotkové submatice řádu r v $\boldsymbol{B}$ nyní hraje horní trojúhelníková submatice $\boldsymbol{U}$ řádu r v $\boldsymbol{S}'$. Konstrukce prostoru $\mathcal{N}(\boldsymbol{A})$ popsaná v důkazu tvrzení 4.29(4) koresponduje s konstrukcí ze 4.40: jestliže $\boldsymbol{U}$ nahradíme jednotkovou maticí $\boldsymbol{I}_r$, tak horní blok $-\boldsymbol{U}^{-1}.\boldsymbol{S}''$ ve vyjádření $\boldsymbol{N}$ přejde v matici $-\boldsymbol{I}_n^{-1}.\boldsymbol{S}'' = -\boldsymbol{S}''$, která koresponduje s maticí $-\boldsymbol{C}'$. Nevýhodou je nutnost vypočítat $-\boldsymbol{U}^{-1}.\boldsymbol{S}''$, což dle (1) odpovídá řešení maticové rovnice $\boldsymbol{U}.\boldsymbol{X} = -\boldsymbol{S}''$.
- Konstrukce LU-rozkladu je konstruktivní, zatímco důkaz 4.22 nikoliv: u konkrétní matice totiž obvykle není snadné určit její sloupcovou bázi pro konstrukci $\boldsymbol{B}$. Teoreticky bychom mohli sice využít 4.39. Mnoho bychom si však nepomohli, protože nalezení $\boldsymbol{C}$ by vyžadovalo řešit vzhledem k $\boldsymbol{C}$ maticovou rovnici $\boldsymbol{A} = \boldsymbol{B}.\boldsymbol{C}$, což opět není snadné, neboť $\boldsymbol{B}$ nemá obecně žádnou speciální strukturu, která by toto usnadnila. Tyto komplikace zdaleka nejsou vyváženy výhodou snadného nalezení báze prostoru $\mathcal{N}(\boldsymbol{A})$, které nevyžaduje řešení žádné inverzní úlohy.

(3) LU-rozklad není jediným užitečným rozkladem skeletního typu. Další hojně využívaný (jen pro $\mathbb{F} \subseteq \mathbb{C}$) je tzv. **QR-rozklad**:

$\boldsymbol{A} = \boldsymbol{Q}.\boldsymbol{R}$. Jeho výhodou je, že sloupce matice $\boldsymbol{Q}$ tvoří ortonormální bázi prostoru $\mathcal{R}(\boldsymbol{A})$, matice $\boldsymbol{R}$ je horní trojúhelníková a dle 4.13a) její sloupce opět představují vektory souřadnic sloupců matice $\boldsymbol{A}$ v ONB dané maticí $\boldsymbol{Q}$. Sloupce $\boldsymbol{Q}$ lze vždy doplnit na ONB celého prostoru $\mathbb{F}^m$ (viz 3.79) a matici $\boldsymbol{R}$ pak stejným počtem nulových řádků. Můžeme tedy bez újmy na obecnosti předpokladat, že $\boldsymbol{Q}$ je unitární matice: analogie s LU-rozkladem, kde regulární matici $\boldsymbol{L}$ můžeme považovat za doplnění sloupcové báze $\boldsymbol{L}'$ prostoru $\mathcal{R}(\boldsymbol{A})$ na bázi celého prostoru $\mathbb{F}^m$.

QR-rozklad se s výhodou užívá místo Gram-Schmidtova algoritmu 3.78 k nalezení ONB prostoru $\mathcal{R}(\boldsymbol{A})$. Ten totiž trpí numerickou nestabilitou v situacích, kdy některý sloupcový vektor matice $\boldsymbol{A}$ je blízký lineární kombinaci ostatních. Při numerických výpočtech se proto doporučuje dávat přednost QR-algoritmu. Teoretické odvození QR-rozkladu jde nad rámec tohoto kurzu. Čtenář jej může najít například ve skriptech [$\mathtt{Šik: odst.\ 13.2\ s.105-110}$].

(4) **Jordanova eliminace** je modifikací Gaussovy eliminace, kdy v matici $\boldsymbol{A}$ eliminujeme postupně nejen pod diagonálou, ale i nad diagonálou. Regulární horní trojúhelníková submatice $S([1,\ldots,r],[j_1,\ldots,j_r])$, ve schodovitém tvaru se tak stane diagonální maticí s nenulovou diagonálou ($r = \mathrm{r}(\boldsymbol{A})$). Můžeme také postupovat tak, že eliminujeme horní části sloupců $S([1,\ldots,i-1],j_i)$, $i = 1,\ldots,r$ ve schodovitém tvaru $\boldsymbol{S}$ až dodatečně. Jestliže každý řádek takto získané diagonální submatice $S([1,\ldots,r],[j_1,\ldots,j_r])$ navíc vydělíme nenulovým diagonálním prvkem s_{ij_i}, $i = 1,\ldots,r$ (neboli násobíme $\boldsymbol{S}$ zleva postupně regulárními transformačními maticemi $\boldsymbol{D}_i^{(1/s_{ij_i})}$ pro $i = 1,\ldots,r$), přejde $S([1,\ldots,r],[j_1,\ldots,j_r])$ dokonce v jednotkovou matici $\boldsymbol{I}_r$.

Výše uvedeným postupem lze tedy každou regulární matici $\boldsymbol{A}$ převést na jednotkovou matici $\boldsymbol{I}_n$, neboť v tomto případě

$r = n$.

Na závěr poznamenejme, že příslušná transformační matice $\boldsymbol{R}$ realizující Jordanovu eliminaci na diagonální tvar (ať obecný či s jednotkovou diagonálou) sice zůstane regulární, ztratí však svůj dolní trojúhelníkový tvar. Podobně v příslušném LU-rozkladu již ani matice $\boldsymbol{L}$ nebude dolní trojúhelníková, ale jen regulární.

Relevantní procedury v MATLABu:

`rref` ... převod matice na schodovitý tvar a určení sloupcové báze (rref=reduced row echelon form)
`lu` ... nalezení LU-rozkladu matice
`qr` ... nalezení QR-rozkladu matice
`orth` ... nalezení ONB prostoru $\mathcal{R}(\boldsymbol{A})$ užitím QR-rozkladu
`null` ... nalezení ONB prostoru $\mathcal{N}(\boldsymbol{A})$.

4.5. **PERMUTACE, DETERMINANT A STOPA MATICE.**

V tomto odstavci zavedeme dvě z nejdůležitějších skalárních veličin přiřazovaných k matici: **determinant** matice a **stopu** matice.

Pojem determinantu patří mezi základní pojmy lineární algebry. V tomto odstavci uvedeme některé jeho základní vlastnosti a metody jeho výpočtu. Poznamenejme, že v dnešní době je praktické použití determinantů na ústupu vzhledem k existenci efektivnějších algoritmů pro řešení úloh, v nichž se tradičně používaly (řešení systému lineárních rovnic, inverze matice aj.) Nicméně pro teoretickou oblast lineární algebry, vyjadřování různých algebraických i geometrických vlastností je pojem determinantu stále nezbytný.
Pojem determinantu se vztahuje ke čtvercovým maticím následovně: Každé čtvercové matici $\boldsymbol{A} = [a_{ij}]$ řádu n je podle přesně uvedeného pravidla (viz dále 4.44) přiřazen skalár z $\mathbb{F}$ (obvykle reálné nebo komplexní číslo) nazývané *determinantem matice* $\boldsymbol{A}$ a označované symboly

$$\det \boldsymbol{A} \qquad \text{nebo} \qquad \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} =: |\boldsymbol{A}|.$$

I když je $\det \boldsymbol{A}$ skalár, užíváme pro determinant názvy týkající se matic a rozumíme jimi názvy pojmů matice $\boldsymbol{A}$. Tak například mluvíme o řádku determinantu, sloupci, hlavní diagonále determinantu a pod. Ke přesné definici determinantu je nezbytné nejprve zavést pojem parity permutace.

DEFINICE 4.42 (Parita permutace `[Šik:odst.2.1 s.12]`).
Nechť σ je permutace nějaké n-prvkové úplně uspořádané množiny J. Bez újmy na obecnosti můžeme předpokládat $J = \{1, 2, \ldots, n\}$. Jestliže označíme $\sigma(i) := \sigma_i$, pak pro permutaci σ budeme používat buď jednořádkový zápis

$$[\sigma] := [\sigma_1, \sigma_2, \ldots, \sigma_n]$$

nebo dvouřádkový zápis

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma_1 & \sigma_2 & \dots & \sigma_n \end{pmatrix} \quad \text{nebo případně} \quad \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix},$$

kde $i_1, i_2, \dots, i_n$ jsou prvky J uspořádané v jiném pořadí a $j_k = \sigma(i_k)$ pro $k = 1, 2, \dots, n$.

Říkáme, že σ_i, σ_j **stojí v inverzi**, jestliže $i < j$ a $\sigma_i > \sigma_j$. Permutace σ se pak nazývá **sudá**, resp. **lichá**, když $(-1)^p = +1$, resp. $(-1)^p = -1$, kde p je počet inverzí permutace σ (neboli když v permutaci σ je sudý, resp. lichý počet navzájem různých dvojic σ_i, σ_j stojících v inverzi). Číslo $\operatorname{sgn}\sigma := (-1)^p$ se pak nazývá **paritou** nebo také **znaménkem** permutace σ.

Jestliže existuje $k > 1$ navzájem různých prvků $K := \{i_1, \dots, i_k\}$ množiny J takových, že $[\sigma_{i_1}, \dots, \sigma_{i_k}]$ představuje permutaci množiny K, pak tuto permutaci nazýváme **cyklem** permutace σ a číslo k délkou cyklu. Cyklům délky 2 se říká **záměna prvků** i_1 **a** i_2.

VĚTA 4.43 (Vlastnosti parity permutace)**.**

(1) *Identická permutace má sudou paritu.*

(2) *Inverzní permutace k permutaci σ má stejnou paritu:* $\operatorname{sgn}\sigma^{-1} = \operatorname{sgn}\sigma$.

(3) *Při skládání permutací se jejich parity násobí:* $\operatorname{sgn}(\sigma_1\sigma_2) = \operatorname{sgn}(\sigma_2\sigma_1) = \operatorname{sgn}\sigma_1 . \operatorname{sgn}\sigma_2$.

(4) *Záměnou dvou různých prvků v jednořádkovém zápisu permutace dostaneme novou permutaci s opačnou paritou (znaménkem).*

(5) *Jsou-li $[\sigma]$ a $[\sigma']$ jednořádkové zápisy dvou permutací, pak jeden z druhého se dá dostat posloupností záměn*[19] *a obě permutace mají stejnou (různou) paritu právě když počet záměn je sudý (lichý).*

(6) *Počet všech permutací je $n!$, přičemž pro $n > 1$ je toto číslo sudé, jedna polovina permutací má sudou paritu a druhá polovina lichou paritu.*

[19] dokonce se můžeme omezit jen na záměny sousedních prvků.

Důkaz.

(1) V identické permutaci nevystupuje žádná inverze $\Rightarrow (-1)^0 = 1$ a parita je tedy sudá.

(2) σ_i, σ_j jsou v inverzi $\Leftrightarrow$ $i < j$ a $k := \sigma_i > \sigma_j =: l$ $\Leftrightarrow$ $l < k$ a $j = \sigma^{-1}(l) > \sigma^{-1}(k) = i$ $\Leftrightarrow$ $\sigma^{-1}(l), \sigma^{-1}(k)$ jsou v inverzi. Tedy σ i σ^{-1} mají stejný počet inverzí a tudíž i stejnou paritu.

(3) Nechť $\sigma := \sigma_2\sigma_1$, p_1 je počet inverzí v σ_1 a p_2 počet inverzí v σ_2. Pak každá z p_2 inverzí permutace σ_2 buď zruší nějakou existující inverzi v σ_1 nebo ji naopak přidá. Protože $(-1)^{p_1+1} = (-1)^{p_1-1}$, bude mít σ paritu $(-1)^{p_1+p_2} = (-1)^{p_1}(-1)^{p_2} = (\operatorname{sgn}\sigma_1)(\operatorname{sgn}\sigma_2)$. Pro $\sigma_1\sigma_2$ analogicky záměnou role σ_1 a σ_2.

(4) Nechť $i < j$ a

$$[\sigma] = [\sigma_1 \dots \sigma_i \dots \sigma_j \dots \sigma_n],\ [\sigma'] = [\sigma_1 \dots \sigma_j \dots \sigma_i \dots \sigma_n].$$

Pokud i, j jsou sousední $(j - i = 1)$, dojde ke změně inverze jen jednou a to u dvojice σ_i, σ_j. Tedy parita permutace se změní. Pokud $j - i > 1$, změní se navíc inverze ještě všech indexů k, kde $i < k < j$, a to jak vzhledem k σ_i, tak vzhledem σ_j. Takových indexů k je $j - i - 1$, takže celkový počet změn je liché číslo $2(j - i - 1) + 1$ a tudíž i v tomto případě dojde ke změně parity permutace.

(5) $[\sigma']$ dostaneme ze $[\sigma]$ následující posloupností záměn: Je-li $\sigma_{i_1} = \sigma'_1$ a $i_1 \neq 1$, pak záměnou σ_1 a σ_{i_1} dosáhneme správného umístění σ'_1 na první pozici. Podobně pro $\sigma_{i_2} = \sigma'_2$ a $i_2 \neq 2$ záměnou σ'_2 a σ_{i_2} umístíme σ'_2 správně na druhou pozici, atd. Každou záměnu na pozicích, které nejsou sousední přitom jistě můžeme nahradit posloupností záměn sousedních prvků.

(6) Pro $n > 1$ je $n! = 1.2\dots$ sudé číslo. Vyberme libovolně nějakou permutaci $\sigma \in \Sigma(J)$. K $[\sigma]$ můžeme dle (4) přiřadit permutaci $[\sigma']$ opačné parity záměnou prvých dvou prvků

v $[\sigma]$. Ze zbylého sudého počtu $n! - 2$ permutací opět analogicky vytvoříme další obdobnou dvojici. Celkem dostaneme $n!/2$ takových dvojic, kde jeden člen má sudou a jeden lichou paritu.

$\square$

DEFINICE 4.44 (Determinant)**.**
Nechť $\boldsymbol{A} =: [a_{ij}]$ je čtvercová matice řádu n a $\Sigma(J)$ množina všech permutací ($\operatorname{card} \Sigma(J) = n!$) množiny jejích sloupcových indexů $J = \{1, 2, \ldots, n\}$. Pak číslo (skalár)

$$\det \boldsymbol{A} := \sum_{\sigma \in \Sigma(J)} (\operatorname{sgn} \sigma) a_{1\sigma_1} \ldots a_{n\sigma_n}$$

nazýváme **determinantem** matice $\boldsymbol{A}$.
Součin $a_{1\sigma_1} \ldots a_{n\sigma_n}$ nazýváme **členem** determinantu a $\operatorname{sgn} \sigma$ jeho **znaménkem**.

Poznámka 4.45. Z definice plyne, že každý člen determinantu se dostane jako součin prvků matice $\boldsymbol{A}$ vybraných přesně po jednom z každého jejího řádku. Podle věty 4.43(6) je počet všech členů $n!$, přičemž pro $n > 1$ jedna polovina z nich má kladné a druhá polovina záporné znaménko.

VĚTA 4.46 (Základní vlastnosti determinantu `[Šik:V2.6 s.14]`)**.**
Nechť $\boldsymbol{A} =: [a_{ij}] =: [\boldsymbol{a}_1; \ldots; \boldsymbol{a}_n]$ je matice řádu n a $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ její řádky. Pak platí

(1) *Obsahuje-li $\boldsymbol{A}$ nulový řádek, pak* $\det \boldsymbol{A} = 0$.
(2) *Je-li $\boldsymbol{b} =: [b_1, \ldots, b_n]$ řádkový vektor, pak pro matici získanou z $\boldsymbol{A}$ přičtením vektoru $\boldsymbol{b}$ k jejímu i-tému řádku $\boldsymbol{a}_i$*

$(i = 1, \dots, n)$ platí:

$$\det \begin{bmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{a}_{i-1} \\ \boldsymbol{a}_i + \boldsymbol{b} \\ \boldsymbol{a}_{i+1} \\ \vdots \\ \boldsymbol{a}_n \end{bmatrix} = \det \underbrace{\begin{bmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{a}_{i-1} \\ \boldsymbol{a}_i \\ \boldsymbol{a}_{i+1} \\ \vdots \\ \boldsymbol{a}_n \end{bmatrix}}_{\boldsymbol{A}} + \det \begin{bmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{a}_{i-1} \\ \boldsymbol{b} \\ \boldsymbol{a}_{i+1} \\ \vdots \\ \boldsymbol{a}_n \end{bmatrix}.$$

(3) *Výměnou dvou různých řádků v matici $\boldsymbol{A}$ se změní znaménko jejího determinantu* $\det \boldsymbol{A}$.

(3a) *Důsledek 1*[20]*: Má-li $\boldsymbol{A}$ dva různé řádky stejné, pak* $\det \boldsymbol{A} = 0$.

(3b) *Důsledek 2: Je-li σ nějaká permutace množiny $\{1, \dots, n\}$ a $\boldsymbol{P}_\sigma$ příslušná permutační matice (viz 4.14(6)), pak* $\det \boldsymbol{P}_\sigma = \operatorname{sgn} \sigma$.
Zejména $\det \boldsymbol{P}_{i,j} = -1$*, kde $\boldsymbol{P}_{i,j}$ je permutační matice řádu n pro záměnu i-ho a j-tého řádku jako v definici 4.33(1).*

(3c) *Důsledek 3:* $\det(\boldsymbol{P}_\sigma \boldsymbol{A}) = \det \boldsymbol{P}_\sigma . \det \boldsymbol{A} = \operatorname{sgn} \sigma . \det \boldsymbol{A}$ *a podobně* $\det(\boldsymbol{A}\boldsymbol{P}_\sigma) = \det \boldsymbol{A} . \det \boldsymbol{P}_\sigma = \operatorname{sgn} \sigma . \det \boldsymbol{A}$.
Zejména $\det(\boldsymbol{P}_{i,j} \boldsymbol{A}) = \det \boldsymbol{P}_{i,j} . \det \boldsymbol{A} = -\det \boldsymbol{A}$ *a podobně* $\det(\boldsymbol{A}\boldsymbol{P}_{i,j}) = \det \boldsymbol{A} . \det \boldsymbol{P}_{i,j} = -\det \boldsymbol{A}$.

(4) *Determinant trojúhelníkové (diagonální) matice je roven součinu jejích prvků v hlavní diagonále.*

(4a) $\det \boldsymbol{I}_n = 1$*, kde $\boldsymbol{I}_n$ je jednotková matice řádu n.*

(5) $\det \boldsymbol{A}^T = \det \boldsymbol{A}$.

(5a) *Důsledek: Všechny výroky této věty týkající se řádků platí i pro sloupce.*

(5b) *Důsledek: V případě $\mathbb{F} \subseteq \mathbb{C}$ platí* $\det \boldsymbol{A}^* = \overline{\det \boldsymbol{A}}$.

---

[20] Toto tvrzení platí jen když pole skalárů $\mathbb{F}$ nemá charakteristiku 2 (srov. 2.71), tedy například pro $\mathbb{F} = \mathbb{R}$ nebo $\mathbb{F} = \mathbb{C}$, což jsou pole nekonečné charakteristiky (viz příklad 2.76).

(6) *Nechť* $\boldsymbol{A}'$ *je matice získaná z* $\boldsymbol{A}$ *vynásobením některého jejího řádku skalárem* α*, pak* $\det \boldsymbol{A}' = \alpha. \det \boldsymbol{A}$.

(6a) *Důsledek 1:* $\det \boldsymbol{D}_i^{(\alpha)} = \alpha$*, kde* $\boldsymbol{D}_i^{(\alpha)}$ *je transformační matice řádu* n *jako v definici 4.33(3).*

(6b) *Důsledek 2:* $\det(\boldsymbol{D}_i^{(\alpha)}\boldsymbol{A}) = \det \boldsymbol{D}_i^{(\alpha)}. \det \boldsymbol{A} = \alpha. \det \boldsymbol{A}$ *a podobně* $\det(\boldsymbol{A}\boldsymbol{D}_i^{(\alpha)}) = \det \boldsymbol{A}. \det \boldsymbol{D}_i^{(\alpha)} = \alpha. \det \boldsymbol{A}$.

(6c) *Důsledek 3:* $\det(\alpha.\boldsymbol{A}) = \alpha^n. \det \boldsymbol{A}$.

(7) $\det \boldsymbol{A}$ *se nemění přičtením* α*-násobku* j*-ho řádku k* i*-tému* $(i \neq j)$.

(7a) *Důsledek 1:* $\det \boldsymbol{R}_{ij}^{(\alpha)} = 1$*, kde* $\boldsymbol{R}_{ij}^{(\alpha)}$ *je transformační matice řádu* n *jako v definici 4.33(2).*

(7b) *Důsledek 2:* $\det(\boldsymbol{R}_{ij}^{(\alpha)}\boldsymbol{A}) = \det \boldsymbol{R}_{ij}^{(\alpha)}. \det \boldsymbol{A} = \det \boldsymbol{A}$ *a podobně* $\det(\boldsymbol{A}\boldsymbol{R}_{ij}^{(\alpha)}) = \det \boldsymbol{A}. \det \boldsymbol{R}_{ij}^{(\alpha)} = \det \boldsymbol{A}$.

(8) *Je-li* $\boldsymbol{R}$ *součin transformačních matice typu* $\boldsymbol{P}_{ij}$*,* $\boldsymbol{R}_{ij}^{(\alpha)}$ *nebo* $\boldsymbol{D}_i^{(\alpha)}$ *pak* $\det(\boldsymbol{R}\boldsymbol{A}) = \det \boldsymbol{R}. \det \boldsymbol{A}$ *a* $\det(\boldsymbol{A}\boldsymbol{R}) = \det \boldsymbol{A}. \det \boldsymbol{R}$.

(8a) *Je-li* $\boldsymbol{T}$ *trojúhelníková (diagonální) matice řádu* n*, pak* $\det(\boldsymbol{T}\boldsymbol{A}) = \det \boldsymbol{T}. \det \boldsymbol{A}$ *a podobně* $\det(\boldsymbol{A}\boldsymbol{T}) = \det \boldsymbol{A}. \det \boldsymbol{T}$.

(9) *Cauchyova věta o determinantu součinu matic: Pro libovolnou čtvercovou matici* $\boldsymbol{B}$ *řádu* n *platí* $\det(\boldsymbol{A}\boldsymbol{B}) = (\det \boldsymbol{A}).(\det \boldsymbol{B})$.

(10) *Matice* $\boldsymbol{A}$ *je regulární (neboli dle 4.18b) má lineárně nezávislé řádky, resp. sloupce) právě když* $\det \boldsymbol{A} \neq 0$.

(11) *Nechť* $\boldsymbol{X}$ *je čtvercová matice, pro niž platí* $\boldsymbol{A}\boldsymbol{X} = \boldsymbol{I}_n$ *(resp.* $\boldsymbol{X}\boldsymbol{A} = \boldsymbol{I}_n$*), pak platí také druhá identita* $\boldsymbol{X}\boldsymbol{A} = \boldsymbol{I}_n$ *(resp.* $\boldsymbol{A}\boldsymbol{X} = \boldsymbol{I}_n$*) a tedy* $\boldsymbol{X} = \boldsymbol{A}^{-1}$ *(viz též větu 4.25)*[21].

(12) *Když* $\boldsymbol{A}^{-1}$ *existuje, pak* $\det \boldsymbol{A}^{-1} = (\det \boldsymbol{A})^{-1}$.

Důkaz.

(1) Nechť $\boldsymbol{a}_i$ je nulový řádek. Pak $\det \boldsymbol{A} := \sum_{\sigma \in \Sigma(J)} (\operatorname{sgn} \sigma) a_{1\sigma_1} \dots a_{i\sigma_i} \dots a_{n\sigma_n} = 0$, neboť $a_{i\sigma_i} = 0$ pro každou permutaci $\sigma \in \Sigma(J)$.

[21]Toto tvrzení říká, že k definici inverzní matice stačí jen jeden z definičních vztahů $\boldsymbol{A}\boldsymbol{X} = \boldsymbol{I}_n$ nebo $\boldsymbol{X}\boldsymbol{A} = \boldsymbol{I}_n$.

(2) Pro determinant na levé straně rovnosti platí vztah:

$$\sum_{\sigma\in\Sigma(J)} (\operatorname{sgn}\sigma) a_{1\sigma_1}\dots(a_{i\sigma_i}+b_{\sigma_i})\dots a_{n\sigma_n} = \sum_{\sigma\in\Sigma(J)} (\operatorname{sgn}\sigma) a_{1\sigma_1}\dots a_{i\sigma_i}\dots a_{n\sigma_n} + \sum_{\sigma\in\Sigma(J)} (\operatorname{sgn}\sigma) a_{1\sigma_1}\dots b_{\sigma_i}\dots a_{n\sigma_n},$$

což je právě součet determinantů matic vpravo.

(3) Nechť $\boldsymbol{B} =: [b_{ij}]$ je matice vzniklá z $\boldsymbol{A}$ záměnou řádků $\boldsymbol{a}_i$ a $\boldsymbol{a}_j$. Pak

$$\det \boldsymbol{B} = \sum_{\sigma\in\Sigma(J)} (\operatorname{sgn}\sigma) b_{1\sigma_1}\dots b_{i\sigma_i}\dots b_{j\sigma_j}\dots b_{n\sigma_n} = \sum_{\sigma\in\Sigma(J)} (\operatorname{sgn}\sigma) a_{1\sigma_1}\dots a_{j\sigma_i}\dots a_{i\sigma_j}\dots a_{n\sigma_n} = \sum_{\sigma'\in\Sigma(J)} (-\operatorname{sgn}\sigma') a_{1\sigma'_1}\dots a_{i\sigma'_i}\dots a_{j\sigma'_j}\dots a_{n\sigma'_n} = -\det \boldsymbol{A},$$

neboť $[\sigma']$ vznikla ze $[\sigma]$ záměnou σ_i a σ_j, takže dle 4.43(4) $\operatorname{sgn}\sigma = -\operatorname{sgn}\sigma'$ ve všech členech determinantu.

(3a) Nechť $\boldsymbol{a}_i = \boldsymbol{a}_j$ pro $i \neq j$. Jejich záměnou se matice nezmění, takže $\det \boldsymbol{A} = \det \boldsymbol{B} \overset{(3)}{=} -\det \boldsymbol{A}$. Odtud $(2 \det \boldsymbol{A}) = 0$ a tedy také $\det \boldsymbol{A} = 0$, pokud $\mathbb{F}$ nemá charakteristiku 2.

(3b) Podle 4.43(5) se $[\sigma]$ dá získat posloupností záměn z identické permutace. Pak dle 4.43(1)(4) $\operatorname{sgn}\sigma = (-1)^p$, kde p je počet takových záměn. Tvrzení je pak důsledkem (3) a (4a): $\boldsymbol{P}_\sigma$ dostaneme z $\boldsymbol{I}_n$ pomocí p řádkových záměn, takže $\det \boldsymbol{P}_\sigma = (-1)^p \det \boldsymbol{I}_n \overset{(4a)}{=} (-1)^p$.

(3c) $\boldsymbol{P}_\sigma \boldsymbol{A}$ je matice získaná z $\boldsymbol{A}$ pomocí p řádkových záměn určujících σ jako ve (3b). Pak $\det(\boldsymbol{P}_\sigma \boldsymbol{A}) \overset{(3)}{=} (-1)^p \det \boldsymbol{A} \overset{(3b)}{=} \det \boldsymbol{P}_\sigma . \det \boldsymbol{A}$.

(4) Člen determinantu dolní trojúhelníkové matice může být nenulový jen když do něj nevybíráme nulové prvky nad hlavní diagonálou. V 1. řádku jediný takový prvek je a_{11}, ve 2. řádku a_{21} již vybrat nelze, takže zbývá a_{22}, atd. až z posledního řádku zbude také jen možnost a_{nn}. Jediný člen který může být nenulový je tedy $a_{11} \dots a_{nn}$, který odpovídá identické permutaci sudé parity. V případě horní trojúhelníkové matice obdobně postupujeme odzdola nahoru.

(4a) Plyne ze (4), neboť jednotková matice je speciální případ diagonální matice.

(5) Označíme-li $\boldsymbol{A}^T =: [a'_{ij}]$, $a'_{ij} := a_{ji}$ a $a := a_{1\sigma_1} \dots a_{n\sigma_n}$ člen determinantu $\det \boldsymbol{A}$, pak $a = a'_{\sigma_1 1} \dots a'_{\sigma_n n} = a_{1\sigma^{-1}(1)} \cdots a_{n\sigma^{-1}(n)}$ je také členem determinantu $\det \boldsymbol{A}^T$ odpovídajícímu permutaci σ^{-1}. Parita obou permutací je stejná dle 4.43(2), takže oba determinanty maji všechny členy stejné včetně znaménka.

(5a) Zřejmé užitím (5).

(5b) $\det \boldsymbol{A}^* \overset{4.10}{=} \det \overline{\boldsymbol{A}^T} \overset{4.44}{=} \overline{\det \boldsymbol{A}^T} \overset{(5)}{=} \overline{\det \boldsymbol{A}}$.

(6) Z každého členu determinatu lze α vytknout a tedy jej lze vytknout i z $\det \boldsymbol{A}$, který je jejich součtem.

(6a) Matice $\det \boldsymbol{D}_i^{(\alpha)}$ vznikla z $\boldsymbol{I}_n$ vynásobením jejího i-ho řádku číslem α. Pak tedy $\det \boldsymbol{D}_i^{(\alpha)} \overset{(6)}{=} \alpha. \det \boldsymbol{I}_n \overset{(4a)}{=} \alpha$.

(6b) Je důsledkem (6) a (6a).

(6c) $\alpha \boldsymbol{A}$ je matice, jejíž každý řádek byl vynásoben číslem α. Stačí aplikovat (6) postupně pro každý z n řádků.

(7) Ve (2) položme $\boldsymbol{b} = \alpha \boldsymbol{a}_j$. Užitím (6) pak poslední sčítanec bude ve tvaru součinu čísla α s determinantem matice, v níž je řádek $\boldsymbol{a}_j$ dvakrát. Podle (3a) je proto nulový a zůstane tak jen prvý sčítanec $\det \boldsymbol{A}$.

(7a) Plyne ze (4a), neboť $\boldsymbol{R}_{ij}^{(\alpha)}$ vznikne z jednotkové matice přičtením α-násobku jejího j-tého řádku k i-tému. Tvrzení plyne také přímo ze (4), neboť $\boldsymbol{R}_{ij}^{(\alpha)}$ je trojúhelníková matice s jednotkovou diagonálou.

(7b) Je důsledkem (7) a (7a).

(8) Dostane se opakovaným užitím (3c), (6b) nebo (7b).

(8a) Nechť $\boldsymbol{T} =: [t_{ij}]$ je například horní trojúhelníková matice. Snadno nahlédneme, že
$\boldsymbol{T} = \boldsymbol{D}_n^{(t_{nn})} \dots \boldsymbol{R}_{2n}^{(t_{2n})} \dots \boldsymbol{R}_{23}^{(t_{23})} \boldsymbol{D}_2^{(t_{22})} \boldsymbol{R}_{1n}^{(t_{1n})} \dots \boldsymbol{R}_{12}^{(t_{12})} \boldsymbol{D}_1^{(t_{11})}$.
Násobení těmito maticemi v pořadí zprava doleva postupně vytváří 1. řádek, pak 2. řádek, atd. až poslední řádek matice $\boldsymbol{T}$. V případě dolní trojúhelníkové matice postupujeme obdobně od posledního řádku k prvnímu. Tvrzení je pak důsledkem (8).

(9) Nechť $\boldsymbol{PA} = \boldsymbol{LU}$ je LU-rozklad matice $\boldsymbol{A}$ dle 4.38. Pak
$\det \boldsymbol{P}. \det(\boldsymbol{AB}) \overset{(3c)}{=} \det(\boldsymbol{PAB}) = \det(\boldsymbol{L}(\boldsymbol{UB})) \overset{(8a)}{=}$
$(\det \boldsymbol{L}. \det \boldsymbol{U}). \det \boldsymbol{B} \overset{(8a)}{=} \det(\boldsymbol{LU}). \det \boldsymbol{B} = \det(\boldsymbol{PA}). \det \boldsymbol{B} \overset{(3c)}{=}$
$\det \boldsymbol{P}. \det \boldsymbol{A}. \det \boldsymbol{B}$. Po zkrácení hodnotou $\det \boldsymbol{P} \overset{(3b)}{=} \pm 1$ dostáváme požadovaný vztah.

(10) Matice $\boldsymbol{A}$ řádu n je podle definice 4.17 regulární $\Leftrightarrow$ $\mathrm{r}(\boldsymbol{A}) = n$ $\overset{4.37}{\Leftrightarrow}$ po Gaussově eliminaci schodovitým tvarem matice $\boldsymbol{A}$ je horní trojúhelníková čtvercová matice $\boldsymbol{S}$ řádu n s nenulovou diagonálou $\Leftrightarrow$ pro schodovitý tvar $\boldsymbol{S} =: [s_{ij}]$ matice $\boldsymbol{A}$ platí $0 \neq s_{11} \dots s_{nn} \overset{(4)}{=} \det \boldsymbol{S} \overset{(3),(7)}{=} \pm \det \boldsymbol{A} \;\Leftrightarrow\; \det \boldsymbol{A} \neq 0$.

(11) Platí-li $\boldsymbol{AX} = \boldsymbol{I}_n$ pro čtvercové matice $\boldsymbol{A}$ a $\boldsymbol{X}$, pak $1 \overset{(4a)}{=} \det \boldsymbol{I}_n = \det(\boldsymbol{AX}) \overset{(9)}{=} (\det \boldsymbol{A})(\det \boldsymbol{X})$. Tedy zejména $\det \boldsymbol{A} \neq 0$ a tudíž podle (10) je matice $\boldsymbol{A}$ regulární a na základě 4.25 k ní existuje inverzní matice $\boldsymbol{A}^{-1}$. Vynásobením rovnice $\boldsymbol{AX} = \boldsymbol{I}_n = \boldsymbol{AA}^{-1}$ zleva maticí $\boldsymbol{A}^{-1}$ obdržíme $\boldsymbol{X} = \boldsymbol{A}^{-1}\boldsymbol{AX} = \boldsymbol{A}^{-1}\boldsymbol{AA}^{-1} = \boldsymbol{A}^{-1}$.

(12) $\boldsymbol{AA}^{-1} = \boldsymbol{I}_n \Rightarrow (\det \boldsymbol{A})(\det \boldsymbol{A}^{-1}) \overset{(9)}{=} \det \boldsymbol{I}_n \overset{(4a)}{=} 1$ a tedy $\det \boldsymbol{A}^{-1} = (\det \boldsymbol{A})^{-1}$.

□

DEFINICE 4.47 (Minory, adjunkt matice).
Nechť $\boldsymbol{A}$ je matice rozměru $m \times n$ a $\boldsymbol{B} = A([i_1, \dots, i_k], [j_1, \dots, j_k])$, $1 \leq i_1 < \cdots < i_k \leq m$, $1 \leq j_1 < \cdots < j_k \leq n$ její čtvercová submatice (viz též definici 4.2) řádu $k \leq \min(m, n)$, pak $\det \boldsymbol{B}$ nazýváme **minorem** (nebo též **subdeterminantem**) řádu k matice $\boldsymbol{A}$. Tento minor budeme značit $M := M^{i_1,\dots,i_k}_{j_1,\dots,j_k}(\boldsymbol{A})$.
Doplňkovým minorem (stručně **doplňkem**) minoru M ve čtvercové matici $\boldsymbol{A}$ řádu n při $k < n$ rozumíme minor složený ze zbývajících řádků a sloupců matice $\boldsymbol{A}$. Značíme jej $C^{i_1,\dots,i_k}_{j_1,\dots,j_k}(\boldsymbol{A})$ nebo jen stručně C. **Algebraický doplněk** minoru M je $\mathcal{C}^{i_1,\dots,i_k}_{j_1,\dots,j_k}(\boldsymbol{A}) := (-1)^s C^{i_1,\dots,i_k}_{j_1,\dots,j_k}(\boldsymbol{A})$, kde $s = i_1 + \cdots + i_k + j_1 + \cdots + j_k$. Je-li minor složen z jediného prvku a_{ij} (tj. $k = 1$, $i_1 = i$ a $j_1 = j$), pak jeho doplněk, resp. algebraický doplněk značíme $C_{ij}(\boldsymbol{A})$, resp. $\mathcal{C}_{ij}(\boldsymbol{A})$. V tomto případě tedy platí $\mathcal{C}_{ij}(\boldsymbol{A}) = (-1)^{i+j} C_{ij}(\boldsymbol{A})$. Matice $\boldsymbol{A}' := [a'_{ij}]$, kde $a'_{ij} = \mathcal{C}_{ji}(\boldsymbol{A})$ se nazývá **adjunktem** k matici $\boldsymbol{A}$ a značí se $\operatorname{adj} \boldsymbol{A}$.

Poznámka 4.48 (Značení).
Pokud nebude hrozit nedorozumění (pevně daná matice $\boldsymbol{A}$), budeme nadále minory matice $\boldsymbol{A}$ a jejich doplňky označovat zjednodušeně $M^{i_1,\dots,i_k}_{j_1,\dots,j_k}$, $C^{i_1,\dots,i_k}_{j_1,\dots,j_k}$, C_{ij}, $\mathcal{C}^{i_1,\dots,i_k}_{j_1,\dots,j_k}$ a $\mathcal{C}_{ij}$ nebo jen M, C a $\mathcal{C}$, pokud rovněž výběrové indexy budou pevně dány.
V dalším budeme v případě čtvercové matice $\boldsymbol{A}$ řádu n pracovat s následujícími výrazy :

$$R(i_1, \dots, i_k) := \sum_{t_1,\dots,t_k} M^{i_1,\dots,i_k}_{t_1,\dots,t_k} \mathcal{C}^{i_1,\dots,i_k}_{t_1,\dots,t_k},$$
$$S(j_1, \dots, j_k) := \sum_{t_1,\dots,t_k} M^{t_1,\dots,t_k}_{j_1,\dots,j_k} \mathcal{C}^{t_1,\dots,t_k}_{j_1,\dots,j_k},$$

kde $t_1, \dots, t_k$ probíhají všechna přirozená čísla s vlastností $1 \leq t_1 < \cdots < t_k \leq n$. Počet sčítanců v každém z výrazů je tedy $\binom{n}{k}$.

<u>VĚTA</u> 4.49 (Laplaceova věta o rozvoji determinantu).
Předpokládejme označení z poznámky 4.48. Pak pro každý výběr řádkových indexů $i_1, \dots, i_k$, resp. sloupcových indexů $j_1, \dots, j_k$ platí

$$R(i_1, \dots, i_k) = S(j_1, \dots, j_k) = \det \boldsymbol{A}.$$

Důkaz. Nechť $M := M^{i_1 \dots i_k}_{j_1 \dots j_k}$ je nějaký minor matice $\boldsymbol{A}$ a $\mathcal{C} = (-1)^s C$ jeho algebraický doplněk, kde $s := \sum_{t=1}^{k} (i_t + j_t)$. Položme $J := \{j_1, \dots, j_k\}$ a $J' := \{1, \dots, n\} - J_1$.
1) Předpokládejme nejprve, že M leží vlevo nahoře ($i_t = j_t = t$), pak $s := \sum_{t=1}^{k} (t + t) = 2(1 + 2 + \dots + k)$ je sudé číslo, takže jeden ze sčítanců $M.\mathcal{C} = M.C$ ve výrazu $R(i_1, \dots, i_k)$ nabude tvaru

$$\begin{aligned} M.C &\overset{4.44}{=} \Big(\sum_{\sigma \in \Sigma(J)} (\operatorname{sgn} \sigma) a_{1\sigma_1} \dots a_{k\sigma_k} \Big) . \Big(\sum_{\sigma' \in \Sigma(J')} (\operatorname{sgn} \sigma') a_{k+1,\sigma'_1} \dots a_{n,\sigma'_{n-k}} \Big) \\ &= \sum_{\sigma \in \Sigma(J)} \sum_{\sigma' \in \Sigma(J')} (\operatorname{sgn} \sigma) a_{1\sigma_1} \dots a_{k\sigma_k} (\operatorname{sgn} \sigma') a_{k+1,\sigma'_1} \dots a_{n,\sigma'_{n-k}} \\ &\overset{4.43(3)}{=} \sum_{\sigma \in \Sigma(J)} \sum_{\sigma' \in \Sigma(J')} (\operatorname{sgn} \sigma\sigma') a_{1\sigma_1} \dots a_{k\sigma_k} a_{k+1,\sigma_{k+1}} \dots a_{n\sigma_n}, \end{aligned}$$

kde $[\sigma\sigma'] = [\sigma_1, \dots, \sigma_k, \sigma_{k+1}, \dots, \sigma_n]$ je permutace množiny $\{1, \dots, n\}$ získaná složením dvou cyklů $[\sigma] =: [\sigma_1, \dots, \sigma_k]$ a $[\sigma'] =: [\sigma'_1, \dots, \sigma'_{n-k}]$, kde $\sigma'_i =: \sigma_{k+i}$ pro $i = 1, \dots, n-k$. Každý ze sčítanců je tedy jedním členem determinantu $d := \det \boldsymbol{A}$ včetně správného znaménka.
2) Nechť nyní minor M je tvořen řádky a sloupci s obecnými indexy $i_1 < \dots < i_k$ a $j_1 < \dots < j_k$. Přemístěme řádky a sloupce (sousedními výměnami) na prvních k pozic tak, aby se zachovalo jejich pořadí. Výměn řádků a sloupců bude celkem

$$(i_1 - 1) + \dots + (i_k - k) + (j_1 - 1) + \dots + (j_k - k) = s - 2(1 + 2 + \dots + k).$$

Výměnami přejde determinant d v nový determinant

$$d' \overset{4.46(3)}{=} (-1)^{s - 2(1+2+\dots+k)} d = (-1)^s d,$$

kde M se přesune do levého horního rohu a jeho doplněk C do pravého dolního rohu. Podle části 1) součin $M.C$ bude roven součtu některých členů determinantu d', opatřených znaménky, která jim přísluší v determinantu d'. Tato znaménka se liší od znamének členů determinantu d jen faktorem $(-1)^s$, takže $M.\mathcal{C} = M.(-1)^s C$ je součet některých členů determinantu d, která jim přísluší v d. Je patrné, že sčítanci v $M.\mathcal{C}$ jsou (formálně) různí a jejich počet je $k!(n-k)!$. Když uvážíme, že lze vybrat $\binom{n}{k}$ minorů z (pevně) zvolených k řádků matice $\boldsymbol{A}$, bude všech sčítanců $k!(n-k)!\binom{n}{k} = k!(n-k)!\frac{n!}{k!(n-k)!} = n!$, tj. celkem součet všech členů determinantu d včetně správných znamének. $\square$

Užijeme-li k výpočtu determinantu matice $\boldsymbol{A}$ výrazu $R(i_1, \ldots, i_k)$ resp. $S(j_1, \ldots, j_k)$, pak řekneme, že jsme jej počítali **Laplaceovým rozvojem podle řádků** $i_1, \ldots, i_k$ **resp. sloupců** $j_1, \ldots, j_k$ nebo že jsme $\det A$ **rozvinuli (Laplaceovým rozvojem) podle řádků** $i_1, \ldots, i_k$ **resp. sloupců** $j_1, \ldots, j_k$.

DŮSLEDEK 4.50 (Laplaceův rozvoj podle jednoho řádku/sloupce)**.**
Nechť i je nějaký řádkový, resp. j sloupcový index. Pak platí

$$\sum_{t=1}^{n} a_{it}\mathcal{C}_{it} = \sum_{t=1}^{n} a_{tj}\mathcal{C}_{tj} = \det \boldsymbol{A}.$$

Lemma 4.51. *Nechť $\boldsymbol{A} = [a_{ij}]$ je čtvercová matice řádu n a nechť $i, j \in \mathbb{N},\ 1 \le i,\ j \le n$. Pak platí:*

(1) $\sum_{t=1}^{n} a_{it}\mathcal{C}_{jt}(\boldsymbol{A}) = \begin{cases} 0, & \textit{jestliže } i \neq j \\ \det \boldsymbol{A}, & \textit{jestliže } i = j, \end{cases}$

(2) $\sum_{t=1}^{n} a_{tj}\mathcal{C}_{ti}(\boldsymbol{A}) = \begin{cases} 0, & \textit{jestliže } i \neq j \\ \det \boldsymbol{A}, & \textit{jestliže } i = j. \end{cases}$

Důkaz.
Jestliže $i = j$, pak výraz (1) je dle 4.50 Laplaceův rozvoj $\det \boldsymbol{A}$ podle i-tého řádku a obdobně výraz (2) Laplaceův rozvoj podle i-tého sloupce.

Jestliže $i \neq j$, pak výraz (1) je dle 4.50 Laplaceův rozvoj podle j-tého řádku determinantu matice, jejíž j-tý řádek byl nahrazen i-tým řádkem. Obdobně výraz (2) představuje Laplaceův rozvoj podle i-tého sloupce determinantu matice, jejíž i-tý sloupec byl nahrazen j-tým sloupcem. Tyto determinanty jsou však podle 4.46(3a) nulové. $\square$

<u>VĚTA</u> 4.52. *Pro čtvercovou matici $\boldsymbol{A}$ řádu n máme:*

$$\boldsymbol{A}(\operatorname{adj} \boldsymbol{A}) = (\operatorname{adj} \boldsymbol{A})\boldsymbol{A} = (\det \boldsymbol{A}).\boldsymbol{I}_n$$

Důkaz.
Tvrzení plyne z lemmatu 4.51 a z definice matice adj $\boldsymbol{A}$ ve 4.47. $\square$

<u>DŮSLEDEK</u> 4.53. *Pro regulární čtvercovou matici $\boldsymbol{A}$ platí*

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

Důkaz. Podle 4.46(10) je $\det \boldsymbol{A} \neq 0$. Rovnici ve 4.52 můžeme tedy tímto determinantem vydělit, takže dostáváme

$$\boldsymbol{A}\Big(\frac{1}{\det \boldsymbol{A}} \operatorname{adj} \boldsymbol{A}\Big) = \Big(\frac{1}{\det \boldsymbol{A}} \operatorname{adj} \boldsymbol{A}\Big)\boldsymbol{A} = \boldsymbol{I}_n,$$

a tedy $\boldsymbol{A}^{-1} = \frac{1}{\det \boldsymbol{A}} \operatorname{adj} \boldsymbol{A}$ podle 4.25. $\square$

<u>DŮSLEDEK</u> 4.54 (Cramerovo pravidlo)**.**
Nechť $\boldsymbol{A}$ je regulární čtvercová matice řádu n a $\boldsymbol{b}$ sloupcový vektor délky n. Pak

$$\boldsymbol{A}^{-1}\boldsymbol{b} = \Big[\frac{\det \boldsymbol{A}_1}{\det \boldsymbol{A}}, \dots, \frac{\det \boldsymbol{A}_n}{\det \boldsymbol{A}}\Big]^T,$$

kde $\boldsymbol{A}_j$ je matice získaná z $\boldsymbol{A}$ nahrazením jejího j-tého sloupce vektorem $\boldsymbol{b}$ $(j = 1, \dots, n)$.

<u>DŮKAZ</u>. Označme $\boldsymbol{b} =: [b_t]$ a položme $\boldsymbol{y} := [y_j] := (\operatorname{adj} \boldsymbol{A})\boldsymbol{b}$. Pak $y_j = \sum_{t=1}^n \mathcal{C}_{tj} b_t = \sum_{t=1}^n b_t \mathcal{C}_{tj}$ představuje Laplaceův rozvoj podle j-tého sloupce determinantu matice $\boldsymbol{A}_j$, tj. $y_j = \det \boldsymbol{A}_j$ $(j = 1, \dots, n)$. Tvrzení pak ihned dostáváme po vynásobení rovnice ve 4.53 zprava vektorem $\boldsymbol{b}$. $\square$

POZNÁMKA 4.55 (Metody výpočtu determinantu).

• **Přímý výpočet z definice 4.44:**
Je vhodný pouze pro matice nízkých řádů, obvykle nejvýše řádu 3:
Řád 1: Pro čtvercovou matici $\boldsymbol{A} = [a]$ řádu 1 je výpočet jednoduchý. Jedinou permutací jednoprvkové množiny je identická permutace sudé parity, takže dostáváme:

$$\det \boldsymbol{A} = \det[a] = a.$$

Řád 2: Jedinými permutacemi dvouprvkové mmnožiny je identická permutace $[1, 2]$ sudé parity a $[2, 1]$ liché parity. Dostáváme tak vztah:

$$\det \boldsymbol{A} = a_{11}a_{22} - a_{12}a_{21}. \tag{4.2a}$$

Řád 3: Tříprvkovou mmnožinu lze uspořádat šesti způsoby $(= 3!)$, přičemž dle 4.43(6) tři permutace mají sudou paritu $(+)$ a tři lichou paritu $(-)$:
$[1, 2, 3], [2, 3, 1], [3, 1, 2]$ s počtem inverzí po řadě $0, 2, 2$ $(+)$
$[3, 2, 1], [2, 1, 3], [1, 3, 2]$ s počtem inverzí po řadě $3, 1, 1$ $(-)$.
Dostáváme tak vztah:

$$\begin{aligned} \det \boldsymbol{A} = {} & a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ & - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}. \end{aligned} \tag{4.2b}$$

Výše uvedené vztahy si lze snadno zapamatovat takto: trojice prvků vybíraná rovnoběžně s hlavní diagonálou dává příslušnému členu znaménko $+$, zatímco trojice prvků vybíraná rovnoběžně s vedlejší diagonálou dává znaménko $-$. Toto pravidlo je také známo jako tzv. **Sarrusovo pravidlo**.

• **Rekurentní výpočet užitím Laplaceova rozvoje:**
Opakovaným používáním Laplaceova rozvoje postupně na zadaný determinant, pak na vybírané minory a jejich doplňky, atd. vede k postupnému snižování řádu determinantů až na úroveň, kde můžeme užít přímý výpočet. Indexy $i_1, \ldots, i_k$, resp. $j_1, \ldots, j_k$ vybíráme tak, aby ve vybraných řádcích, resp. sloupcích bylo co nejvíce nulových

prvků. Pak totiž mnoho minorů v rozvoji bude nulových a výpočet se zjednoduší. Můžeme také tomu napomoci prováděním vhodných elementárních transformací dle 4.46(7-7b), které nemění hodnotu počítaného determinantu.
Obvykle se provádí rozvoj pouze podle jednoho řádku, resp. sloupce, z něhož nejprve eliminujeme co nejvíce nenulových prvků. Ideální je, když tam zůstane pouze jeden takový prvek, řekněme a_{ij}. Pak se rozvoj redukuje jen na jeden sčítanec $\det \boldsymbol{A} = a_{ij}(-1)^{i+j}C_{ij}$, kde C_{ij} je řádu $n-1$. Na něj pak aplikujeme podobný postup, čímž se řád dále sníží na $n-2$, atd.

• **Užití Gaussovy eliminace, resp. LU-rozkladu:**
Při Gaussově eliminaci se matice $\boldsymbol{A}$ řádu n převede posloupností elementárních řádkových úprav 4.46(7) a řádkových záměn 4.46(3) na čtvercovou matici ve schodovitém tvaru $\boldsymbol{S}$ rovněž řádu n. Uvažme dále, že $\boldsymbol{S}$ je horní trojúhelníková matice. Zatímco řádkové úpravy 4.46(7) nemění hodnotu $\det \boldsymbol{A}$, tak každá řádková záměna 4.46(3) obrací její znaménko. Označíme-li p počet provedených řádkových záměn, dostáváme $(-1)^p \det \boldsymbol{A} = \det \boldsymbol{S} \overset{4.46(4)}{=} s_{11} \dots s_{nn}$ a odtud hledaný vztah

$$\det \boldsymbol{A} = (-1)^p s_{11} \dots s_{nn}. \tag{4.3}$$

Obdobný vztah dostáváme z rovnice $\boldsymbol{L}.\boldsymbol{S} = \boldsymbol{P}\boldsymbol{A}$ pro LU-rozklad dle 4.38. Totiž $\boldsymbol{L}$ je dolní trojúhelníková s jednotkovou diagonálou, takže $\det \boldsymbol{L} = 1$ dle 4.46(4). Matice $\boldsymbol{P}$ je permutační matice složená z výše zmíněných řádkových záměn, takže $\det \boldsymbol{P} = (-1)^p$ dle 4.43(3) a 4.46(3b).

Kromě determinantu, další běžně užívanou skalární veličinou přiřazovanou čtvercové matici je stopa matice:

<u>DEFINICE</u> 4.56 (Stopa matice)**.**
Stopou (angl. *trace*) čtvercové matice $\boldsymbol{A} =: [a_{ij}]$ řádu n nazýváme součet jejích prvků na hlavní diagonále. Píšeme $\operatorname{tr} \boldsymbol{A} := \sum_{i=1}^{n} a_{ii}$.

V teorii polynomů hraje důležitou roli tzv. Vandermondova matice:

<u>DEFINICE</u> 4.57 (Vandermondova matice).
Vandermondovou maticí danou vektorem $\boldsymbol{x} := [x_1, \dots, x_n] \in \mathbb{F}^n$ rozumíme následující čtvercovou matici řádu n:

$$\boldsymbol{V}(\boldsymbol{x}) := \boldsymbol{V}(x_1, \dots, x_n) := \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{bmatrix}. \tag{4.4a}$$

V jejím i-tém řádku a j-tém sloupci se nachází prvek x_i^{j-1}, můžeme proto psát stručně[22] $\boldsymbol{V}(\boldsymbol{x}) = [x_i^{j-1}]$.

<u>VĚTA</u> 4.58 (Vandermondův determinant).
Determinant z Vandermondovy matice se nazývá **Vandermondův determinant**. *Vandermondův determinant řádu $n \geq 2$ se spočte z následujícího vztahu:*

$$\det \boldsymbol{V}(x_1, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_j - x_i). \tag{4.4b}$$

DŮKAZ. Důkaz probíhá indukcí vzhledem k n.
1) <u>n=2</u>: užitím (4.2a) ihned dostáváme

$$\det \boldsymbol{V}(x_1, x_2) = \begin{vmatrix} 1 & x_1 \\ 1 & x_2 \end{vmatrix} = 1.x_2 - x_1.1 = x_2 - x_1 = \prod_{1 \leq i < j \leq 2} (x_j - x_i).$$

2) <u>$n > 2$ (indukční krok)</u>: Předpokládejme, že (4.4b) již bylo dokázáno pro $n-1$. Proveďme s maticí (4.4a) následující sloupcové úpravy neměnící hodnotu determinantu (viz 4.46(5a)(7)):
Pro každé $j = n, n-1, \dots, 2$ odečteme od j-tého sloupce x_n-násobek $(j-1)$-ho sloupce. V posledním řádku zůstane v 1. sloupci jediný nenulový prvek 1, podle něhož determinant rozvineme:
$\det \boldsymbol{V}(x_1, \dots, x_n) = 1.(-1)^{n+1} \det \boldsymbol{C}$, kde z každého řádku determinantu doplňkové matice $\boldsymbol{C}$ lze před něj vytknout rozdíl $(x_i - x_n)$,

[22] pokud $x_i = 0$, pak v 1. sloupci neurčitý výraz 0^0 nahradíme jedničkou.

$i = 1, \dots, n-1$ (užijeme $(n-1)$-krát vlastnost 4.46(6)). Pak

$$\det \boldsymbol{C} = (x_1 - x_n) \dots (x_{n-1} - x_n) \det \boldsymbol{V}(x_1, \dots, x_{n-1}) \stackrel{I.P.}{=}$$
$$(-1)^{n-1} (x_n - x_1) \dots (x_n - x_{n-1}) \prod_{1 \le i < j \le n-1} (x_j - x_i) =$$
$$(-1)^{n-1} \prod_{1 \le i < j \le n} (x_j - x_i).$$

Po dosazení do výše uvedeného vztahu dostáváme požadované:
$\boldsymbol{V}(x_1, \dots, x_n) = (-1)^{2n} \prod_{1 \le i < j \le n} (x_j - x_i) = \prod_{1 \le i < j \le n} (x_j - x_i)$. $\square$

<u>**DŮSLEDEK**</u> **4.59.** *Vandermondova matice $\boldsymbol{V}(x_1, \dots, x_n)$ je regulární právě když skaláry $x_1, \dots, x_n$ jsou navzájem různé.*

ANGLICKÁ TERMINOLOGIE TEORIE MATIC

(prázdná, čtvercová) matice ⧫ (empty, square) matrix (pl. matrices)
rozměr (typ) matice ⧫ size of a matrix
prvek ⧫ element
dolní/horní index ⧫ lower/upper subscript (index, pl. indices)
řádek/sloupec ⧫ row/column
submatice ⧫ submatrix
jednotková matice ⧫ identity matrix
hlavní (vedlejší) diagonála ⧫ main (secondary) diagonal
hermitovská (anti)symetrie ⧫ hermitian (anti)symmetry
dolní/horní trojúhelníková ⧫ lower/upper triangular
schodovitý tvar ⧫ reduced row echelon form
(konjugovaná) transpozice ⧫ (complex conjugate) transpose
maticový součin ⧫ matrix product
pravidlo smíšeného součinu ⧫ mixed-product rule
hodnost ⧫ rank
singulární, regulární ⧫ singular, nonsingular
řádkově (sloupcově) plná hodnost ⧫ full-row (full-column) rank
skeletní rozklad ⧫ rank factorization
inverze matice ⧫ matrix inverse
pozitivně (semi)definitní ⧫ positively (nonnegatively) definite
LU-rozklad, QR-rozklad ⧫ LU-factorization, QR-factorization
Gaussian (Jordan) elimination ⧫ Gaussian (Jordan) elimination
permutace, záměna ⧫ permutation, interchange
parita, znaménko, cykl ⧫ parity, sign, cycle
determinant, subdeterminant ⧫ determinant, subdeterminant
(doplňkový) minor ⧫ (complementary) minor
adjunkt matice ⧫ compound matrix
Laplaceův rozvoj ⧫ Laplace expansion
Vandermondova matice ⧫ Vandermonde matrix
Cramerovo pravidlo ⧫ Cramer rule
stopa ⧫ trace
0

5. Řešení systému lineárních rovnic

Teorie a příklady: `[KaSk:odst.10 s.88-99]`, `[Šik:kap.4 s.37-41]`
Příklady: `[Ho:řešené č.24-35; s.24-36]`,
`[Ho:neřešené kap.5 s.126-137]`

Formulace problému:
Je dán systém m lineárních rovnic (SLR) o n neznámých $x_1, x_2, \ldots, x_n$ ve tvaru:

$$\begin{array}{ccccccccccl} a_{11}x_1 & + & a_{12}x_2 & + & \ldots & + & a_{1n}x_n & = & b_1 & \ldots & \text{1. rovnice} \\ a_{21}x_1 & + & a_{22}x_2 & + & \ldots & + & a_{2n}x_n & = & b_2 & \ldots & \text{2. rovnice} \\ \vdots & & \vdots & & \ldots & & \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \ldots & + & a_{mn}x_n & = & b_m & \ldots & m\text{-tá rov.} \end{array} \tag{5.1a}$$

Ekvivalentní maticový zápis systému (5.1a):

$$\boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}, \tag{5.1b}$$

kde je

$\boldsymbol{A} := [a_{ij}]_{\substack{1\le i\le m\\ 1\le j\le n}}$ ... **matice SLR** (5.1a), $a_{ij} \in \mathbb{F}$

$\boldsymbol{b} := \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$ ... **pravá strana** SLR (5.1a), $b_i \in \mathbb{F}$

$\boldsymbol{x} := \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$ ... **vektor neznámých** SLR (5.1a), $x_j \in \mathbb{F}$.

Každý vektor $\boldsymbol{x} \in \mathbb{F}$ vyhovující všem rovnicím SLR (5.1a) nazýváme jeho **řešením**.
Systém rovnic (5.1a) se nazývá **homogenní**, jestliže má nulovou pravou stranu: $\boldsymbol{b} = \mathbf{0}_{m,1}$.

<u>DEFINICE</u> 5.1. Nechť $\boldsymbol{A}$ je matice SLR (5.1b), pak matici $\widetilde{\boldsymbol{A}} := [\boldsymbol{A}, \boldsymbol{b}]$ rozměru $m \times (n+1)$ nazýváme **rozšířenou maticí** tohoto systému. Zřejmě každý SLR je jednoznačně popsán svou rozšířenou maticí soustavy $\widetilde{\boldsymbol{A}}$.

<u>VĚTA</u> 5.2 (Věta o řešitelnosti SLR: **Frobeniova věta**[23])**.**
Systém lineárních rovnic (5.1b) *je řešitelný právě když* $\mathrm{r}(\boldsymbol{A}) = \mathrm{r}(\widetilde{\boldsymbol{A}})$.

<u>DŮKAZ</u>. Systém je řešitelný $\Leftrightarrow$ $\boldsymbol{b} \in \mathcal{R}(\boldsymbol{A}) \overset{4.15(3)}{\Leftrightarrow}$ $\boldsymbol{b}$ je lineární kombinací sloupců matice $\boldsymbol{A} \overset{3.14(5)}{\Leftrightarrow}$ přidáním $\boldsymbol{b}$ ke sloupcům matice $\boldsymbol{A}$ se nemění jimi generovaný prostor $\Leftrightarrow$ $\mathcal{R}(\boldsymbol{A}) = \mathcal{R}(\widetilde{\boldsymbol{A}}) \overset{3.24(3)}{\Leftrightarrow}$ $\dim \mathcal{R}(\boldsymbol{A}) = \dim \mathcal{R}(\widetilde{\boldsymbol{A}}) \overset{4.17}{\Leftrightarrow} \mathrm{r}(\boldsymbol{A}) = \mathrm{r}(\widetilde{\boldsymbol{A}})$. □

<u>DŮSLEDEK</u> 5.3 (Popis množiny všech řešení)**.**
Homogenní SLR s libovolnou maticí soustavy $\boldsymbol{A}$ *je vždy řešitelný a množinou všech jeho řešení je jádro* $\mathcal{N}(\boldsymbol{A})$. *Je-li* $\boldsymbol{x}^{(0)}$ *nějaké řešení (řešitelného) systému* (5.1b), *pak* $\boldsymbol{x}^{(0)}$ *se nazývá jeho* **partikulárním řešením** *a* $\boldsymbol{x}^{(0)} + \mathcal{N}(\boldsymbol{A}) = \{\boldsymbol{x}^{(0)} + \boldsymbol{u} \mid \boldsymbol{u} \in \mathcal{N}(A)\}$ *udává množinu všech jeho řešení. Zejména platí:*

(1) *Systém má jediné řešení právě když* $\mathrm{r}(\boldsymbol{A}) = \mathrm{r}(\widetilde{\boldsymbol{A}}) = n$ *neboli právě když* $\boldsymbol{A}$ *je sloupcově plné hodnosti, ale* $\widetilde{\boldsymbol{A}}$ *nikoliv. Zejména každý systém s regulární maticí soustavy* $(m = n)$ *má vždy právě jedno řešení.*
(2) *Systém má nekonečně mnoho řešení právě když* $r := \mathrm{r}(\boldsymbol{A}) = \mathrm{r}(\widetilde{\boldsymbol{A}})$ *a* $r < n$. *V tomto případě množina všech řešení je tvaru* $\{\boldsymbol{x}^{(0)} + t_1 \boldsymbol{u}^{(1)} + \cdots + t_{n-r} \boldsymbol{u}^{(n-r)} \mid t_1, \ldots, t_{n-r} \in \mathbb{F}\}$, *kde* $\boldsymbol{u}^{(1)}, \ldots, \boldsymbol{u}^{(n-r)}$ *je nějaká báze v* $\mathcal{N}(\boldsymbol{A})$ *a* $t_1, \ldots, t_{n-r} \in \mathbb{F}$ *jsou tzv.* **volné parametry**.

[23]nebo též Kronecker–Capelliho věta.

DŮKAZ.
a) Homogenní systém: $\boldsymbol{x}$ je řešení homogenního systému $\Leftrightarrow$ $\boldsymbol{Ax} = \boldsymbol{0}$ $\overset{3.29}{\Leftrightarrow}$ $\boldsymbol{x} \in \mathcal{N}(\boldsymbol{A})$.
b) Nehomogenní systém: $\boldsymbol{x}$ je řešení nehomogenního systému $\Leftrightarrow$ $\boldsymbol{Ax} = \boldsymbol{b} = \boldsymbol{Ax}^{(0)} \;\Leftrightarrow\; \boldsymbol{Ax} - \boldsymbol{Ax}^{(0)} = \boldsymbol{0} \;\Leftrightarrow\; \boldsymbol{A}(\boldsymbol{x} - \boldsymbol{x}^{(0)}) = \boldsymbol{0} \overset{a)}{\Leftrightarrow}$ $\boldsymbol{x} - \boldsymbol{x}^{(0)} =: \boldsymbol{u} \in \mathcal{N}(\boldsymbol{A}) \;\Leftrightarrow\; \boldsymbol{x} = \boldsymbol{x}^{(0)} + \boldsymbol{u}$, kde $\boldsymbol{u} \in \mathcal{N}(\boldsymbol{A})$.
Poznamenejme, že výše uvedená úvaha koresponduje s teorií o faktor prostorech z odst. 3.5 (věta 3.39 a její důsledky). Totiž $\boldsymbol{A} : \mathbb{F}^n \to \mathbb{F}^m$ určuje dle 4.15 lineární operátor, přičemž množina všech řešení je úplný vzor $\boldsymbol{A}^{-1}(\{\boldsymbol{b}\})$, což je právě jedna ze tříd faktor prostoru $\mathbb{F}^n/\mathcal{N}(\boldsymbol{A})$ (viz 3.41), která se dle 3.40 dá psát ve tvaru $\boldsymbol{x}^{(0)} + \mathcal{N}(\boldsymbol{A})$ pro libovolný reprezentant $\boldsymbol{x}^{(0)}$ této třídy. Podle 4.29(4) je $\dim \mathcal{N}(\boldsymbol{A}) = n - \mathrm{r}(\boldsymbol{A})$. Odtud ihned dostáváme:

(1) Řešitelný systém (podmínka $\mathrm{r}(\boldsymbol{A}) = \mathrm{r}(\widetilde{\boldsymbol{A}})$ z věty 5.2) má tedy právě jedno řešení pouze v případě, že $\mathcal{N}(\boldsymbol{A}) = \{\boldsymbol{0}\}$, tj. když $0 = \dim \mathcal{N}(\boldsymbol{A}) = n - \mathrm{r}(\boldsymbol{A})$, neboli když současně platí $\mathrm{r}(\boldsymbol{A}) = n$. Partikulární řešení $\boldsymbol{x}^{(0)}$ je pak tímto jediným řešením.
(2) V opačném případě ($r := \mathrm{r}(\boldsymbol{A}) < n$) má vždy nekonečně mnoho řešení vyjádřitelných ve tvaru součtu partikulárního řešení $\boldsymbol{x}^{(0)}$ se všemi prvky z jádra $\mathcal{N}(\boldsymbol{A})$, neboli se všemi možnými lineárními kombinacemi vhodně zvolených bázových vektorů $\boldsymbol{u}^{(1)}, \dots, \boldsymbol{u}^{(n-r)} \in \mathcal{N}(\boldsymbol{A})$.

□

DEFINICE 5.4. Řekneme, že dva SLR $\boldsymbol{Ax} = \boldsymbol{b}$ a $\boldsymbol{A}'\boldsymbol{x} = \boldsymbol{b}'$ jsou **ekvivalentní**, jestliže oba systémy mají tytéž množiny řešení. V takovém případě píšeme $\widetilde{\boldsymbol{A}} \sim \widetilde{\boldsymbol{A}}'$, kde $\widetilde{\boldsymbol{A}} := [\boldsymbol{A}, \boldsymbol{b}]$ a $\widetilde{\boldsymbol{A}}' := [\boldsymbol{A}', \boldsymbol{b}']$ značí příslušné rozšířené matice těchto systémů (s týmž počtem sloupců).

Poznámka 5.5 (Princip konstrukce množiny všech řešení SLR).
Základní princip se opírá o nalezení ekvivalentního systému s podstatně jednodušší maticí soustavy, obvykle trojúhelníkové, nebo ještě

lépe diagonální (viz dále). Zde hraje důležitou roli skeletní rozklad matice (věta 4.22). Nechť totiž $\boldsymbol{A} = \boldsymbol{B}\boldsymbol{C}$ je nějaký skeletní rozklad matice soustavy $\boldsymbol{A}$ typu $m \times n$ o hodnosti r. Doplňme zprava lineárně nezávislé sloupce $\boldsymbol{B}$ na bázi v $\mathbb{F}^m$. To lze vždy udělat dle 3.24(1). Obdržíme tak čtvercovou regulární matici $\boldsymbol{B}'$. Jestliže jako $\boldsymbol{C}'$ označíme matici vzniklou z $\boldsymbol{C}$ přidáním $m-r$ nulových řádků zdola, dostáváme $\boldsymbol{A} = \boldsymbol{B}\boldsymbol{C} = \boldsymbol{B}'\boldsymbol{C}'$. Označíme-li $\boldsymbol{T} := \boldsymbol{B}'^{-1}$, pak $\boldsymbol{T}\boldsymbol{A} = \boldsymbol{C}'$. Pak $\boldsymbol{x}$ je řešení SLR $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{b} \;\Leftrightarrow\; \boldsymbol{T}\boldsymbol{A}\boldsymbol{x} = \boldsymbol{T}\boldsymbol{b} \;\Leftrightarrow\; \boldsymbol{C}'\boldsymbol{x} = \boldsymbol{b}'$, kde $\boldsymbol{b}' := \boldsymbol{T}\boldsymbol{b}$. Tedy $[\boldsymbol{A}, \boldsymbol{b}] \sim [\boldsymbol{C}', \boldsymbol{b}']$ určují ekvivalentní systémy, přičemž $[\boldsymbol{C}', \boldsymbol{b}'] = [\boldsymbol{T}\boldsymbol{A}, \boldsymbol{T}\boldsymbol{b}] = \boldsymbol{T}[\boldsymbol{A}, \boldsymbol{b}] = \boldsymbol{T}\widetilde{\boldsymbol{A}}$. Rozšířenou matici ekvivalentního systému tedy dostaneme vynásobením původní rozšířené matice $\widetilde{\boldsymbol{A}}$ zleva regulární transformační maticí $\boldsymbol{T}$.

Typickými rozklady skeletního typu jsou LU-rozklad a QR-rozklad (viz 4.41(2),(3)), kde $\boldsymbol{C}'$ vždy obsahuje regulární horní trojúhelníkovou submatici, která umožňuje snadné nalezení jak partikulárního řešení, tak i báze jádra $\mathcal{N}(\boldsymbol{C}')$, což umožňuje popsat všechna řešení na základě 5.3. Báze jádra se hledá analogicky jako v důkazu 4.29(4)— viz též 4.41(1). V případě LU-rozkladu $\boldsymbol{P}\boldsymbol{A} = \boldsymbol{L}\boldsymbol{S}$ matice $\boldsymbol{T} = \boldsymbol{L}^{-1}\boldsymbol{P}$ odpovídá elementárním řádkovým úpravám převádějícím $\boldsymbol{A}$ na schodovitý tvar $\boldsymbol{C}' =: \boldsymbol{S}$, resp. $\widetilde{\boldsymbol{A}}$ na schodovitý tvar $[\boldsymbol{S}, \boldsymbol{b}']$. V případě QR-rozkladu je $\boldsymbol{B}' =: \boldsymbol{Q}$ unitární matice (viz 4.15(8)) a $\boldsymbol{C}' =: \boldsymbol{R}$, takže dle 3.90(5) roli $\boldsymbol{T} = \boldsymbol{Q}^{-1}$ hraje (hermitovsky) transponovaná matice $\boldsymbol{Q}^*$.

V dalším se soustředíme na metody konstrukce množiny všech řešení založené na LU-rozkladu. V případě QR-rozkladu se postupuje analogicky.

5.1. **SLR s regulární trojúhelníkovou maticí $\boldsymbol{A}$ řádu n.**

Podle 4.27 má $\boldsymbol{A}$ na hlavní diagonále všechny prvky nenulové:
$a_{kk} \neq 0$ pro $k = 1, 2, \ldots, n$.

(1) $\boldsymbol{A}$ dolní trojúhelníková: Algoritmus dopředného dosazování:

$$\boxed{\begin{array}{lcl} x_1 &=& b_1/a_{11} \\ x_k &=& \left(b_k - \sum_{j=1}^{k-1} a_{kj}x_j\right)/a_{kk} \text{ pro } k = 2, 3 \ldots, n. \end{array}} \tag{5.2a}$$

(2) $\boldsymbol{A}$ horní trojúhelníková: Algoritmus zpětného dosazování:

$$\boxed{\begin{array}{lcl} x_n &=& b_n/a_{nn} \\ x_k &=& \left(b_k - \sum_{j=k+1}^{n} a_{kj}x_j\right)/a_{kk} \text{ pro } k = n-1, n-2, \ldots, 1. \end{array}} \tag{5.2b}$$

5.6. Výpočetní složitost algoritmů (5.2a) **a** (5.2b)**.**
Označíme-li $\mathcal{O}(\pm)$ počet operací sečítání a odčítání (aditivní složitost) a $\mathcal{O}(*, /)$ počet operací násobení a dělení (multiplikativní složitost), pak užitím známého vztahu pro součet členů aritmetické posloupnosti dostáváme pro algoritmy dopředného a zpětného dosazování kvadratickou aditivní i multiplikativní složitost:

Aditivní složitost:

$$\mathcal{O}(\pm) = 0 + 1 + \ldots n - 1 = \frac{n(n-1)}{2} = \boxed{\frac{n^2 - n}{2}}.$$

Multiplikativní složitost:

$$\mathcal{O}(*, /) = 1 + 2 + \ldots n = \frac{n(n+1)}{2} = \boxed{\frac{n^2 + n}{2}}.$$

Pokud matice $\boldsymbol{A}$ má jednotkovou diagonálu ($a_{k,k} = 1$ pro $k = 1, 2, \ldots, n$), pak v každém kroku ušetříme jedno dělení a multiplikativní i aditivní složitost bude stejná:

$$\mathcal{O}(*, /) = 0 + 1 + \ldots n - 1 = \mathcal{O}(\pm) = \boxed{\frac{n^2 - n}{2}}.$$

5.2. **SLR s libovolnou maticí soustavy $\boldsymbol{A}$ rozměru $m \times n$.**

(1) Gaussova eliminace

a) Převod $\widetilde{\boldsymbol{A}}$ na schodovitý tvar algoritmem Gaussovy eliminace

Pomocí elementárních řádkových úprav převedeme rozšířenou matici soustavy $\widetilde{\boldsymbol{A}} = [\boldsymbol{A}, \boldsymbol{b}]$ na schodovitý tvar jako v 4.37. Z hlediska numerické přesnosti se doporučuje tzv. **pivotování**, kdy pro přehození řádků vybíráme takový, který má v eliminovaném sloupci prvek co největší v absolutní hodnotě. Při eliminaci se totiž tímto prvkem dělí. Jeho malé (i když nenulové) hodnoty mohou vést k extrémně vysokým hodnotám podílů a tudíž ke ztrátě platných cifer při jejich ukládání v paměti počítače.
Nechť $\boldsymbol{R}$ (=: $\boldsymbol{T}$ v poznámce 5.5) je regulární transformační matice realizující tento převod. Obdržíme:
$\boldsymbol{R}\widetilde{\boldsymbol{A}} = [\boldsymbol{S}, \boldsymbol{b}'] =: \widetilde{\boldsymbol{S}}$, kde $\boldsymbol{S} = \boldsymbol{R}\boldsymbol{A}$ a $\boldsymbol{b}' = \boldsymbol{R}\boldsymbol{b}$.
Podle poznámky 5.5 jsme takto obdrželi ekvivalentní SLR $\boldsymbol{S}\boldsymbol{x} = \boldsymbol{b}'$.

b) Rozhodnutí o řešitelnosti SLR $\boldsymbol{S}\boldsymbol{x} = \boldsymbol{b}'$
Podle Frobeniovy věty 5.2 je tento systém řešitelný právě když $\mathrm{r}(\boldsymbol{S}) = \mathrm{r}(\widetilde{\boldsymbol{S}})$. Uvážíme-li, že $\boldsymbol{S}$ je schodovitý tvar původní matice $\boldsymbol{A}$, tak systém bude řešitelný právě když $\boldsymbol{S}$ i $\widetilde{\boldsymbol{S}}$ mají shodný počet nenulových řádků, který pak udává jejich společnou hodnost r dle 4.30: sloupec $\boldsymbol{b}'$ nepřináší schod navíc.
Je-li systém řešitelný pokračujeme dalším krokem c). Přitom posledních $m - r$ nulových řádků v $\widetilde{\boldsymbol{S}}$ můžeme vynechat, neboť reprezentují rovnice s nulovými koeficienty a nulovými pravými stranami, které

jsou triviálně splněny. Položíme-li tedy $\boldsymbol{S}' := S([1,\dots,r],:)$ a původní $\boldsymbol{b}'$ nahradíme subvektorem $\boldsymbol{b}' = [b_1,\dots,b_r]$ bez $m-r$ koncových nul, pak $\boldsymbol{S}'\boldsymbol{x} = \boldsymbol{b}'$ představuje rovněž SLR ekvivalentní k původnímu.

c) Nalezení partikulárního řešení $\boldsymbol{x}^{(0)}$ systému $\boldsymbol{S}'\boldsymbol{x} = \boldsymbol{b}'$

V matici $\boldsymbol{S}'$, která je rozměru $r \times n$, vyberme sloupcové indexy $1 \le j_1 < \cdots < j_r \le n$ odpovídající sloupcům se schody (viz 4.37). Pak $\boldsymbol{U} := S'(:,[j_1,\dots,j_r])$ je regulární horní trojúhelníková submatice. Nastanou dva případy

(i) $r = n$, kdy $\boldsymbol{U} = \boldsymbol{S}'$ a systém $\boldsymbol{U}\boldsymbol{x} = \boldsymbol{b}'$ má tedy dle 5.3(2) jediné (partikulární) řešení $\boldsymbol{x}^{(0)}$, které nalezneme algoritmem zpětného dosazování (5.2b). Vektor $\boldsymbol{x}^{(0)}$ je také jediným řešením $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}$ a jsme tedy u konce.

(ii) $r < n$, kdy $\boldsymbol{U}$ je vlastní submatice $\boldsymbol{S}'$.
Označme $1 \le k_1 < \cdots < k_{n-r} \le n$ zbývající sloupce v $\boldsymbol{S}'$ a $\boldsymbol{U}'$ matici jimi vytvořenou. Dále nechť $y_p := x_{j_p}$ značí složky $\boldsymbol{x}$ odpovídající sloupcům $\boldsymbol{U}$ (tzv. **vázané proměnné**) a podobně $t_q := x_{k_q}$ zbývající složky (tzv. **volné proměnné**). Pak

$$\begin{aligned} \boldsymbol{b}' = \boldsymbol{S}'\boldsymbol{x} = \sum_{j=1}^{n} S'(:,j)x_j = \sum_{p=1}^{r} S'(:,j_p)y_p + \sum_{q=1}^{n-r} S'(:,k_q)t_q = \\ = \boldsymbol{U}\boldsymbol{y} + \boldsymbol{U}'\boldsymbol{t} \qquad \text{a odtud} \end{aligned}$$

$$\boldsymbol{U}\boldsymbol{y} = \boldsymbol{b}' - \boldsymbol{U}'\boldsymbol{t}. \tag{5.3}$$

Dosadíme-li za všechny volné proměnné nuly, pak $\boldsymbol{t} = \boldsymbol{0}$ a (5.3) přejde v rovnici $\boldsymbol{U}\boldsymbol{y} = \boldsymbol{b}'$, z níž určíme vázané proměnné algoritmem zpětného dosazování jako v (i). Partikulární řešení $\boldsymbol{x}^{(0)}$ tak má složky
$$x_j^{(0)} = \begin{cases} y_p & \text{jestliže } j = j_p \text{ pro nějaké } p \text{ a} \\ 0 & \text{jestliže } j = k_q \text{ pro nějaké } q. \end{cases}$$
Ve většině praktických úloh vystačíme s partikulárním řešením. V opačném případě pokračujeme krokem d).

Poznámka: Pomocí systému MATLAB lze partikulární řešení s nejméně $n-r$ nulovými složkami snadno nalézt užitím operátoru (\) levého dělení: $\boldsymbol{x}^{(0)} = \boldsymbol{S}'\backslash\boldsymbol{b}'$. Pokud $\boldsymbol{A}$ není singulární čtvercová matice, lze jej aplikovat přímo na původní systém: $\boldsymbol{x}^{(0)} = \boldsymbol{A}\backslash\boldsymbol{b}$. V případě singulární čtvercové matice stačí k systému přidat jednu nulovou rovnici. Dostaneme ekvivalentní systém s obdélníkovou maticí soustavy, s níž už lze výše uvedený postup použít.

d) Nalezení báze $\mathcal{N}(\boldsymbol{S}')$ pro popis všech řešení systému $\boldsymbol{S}'\boldsymbol{x} = \boldsymbol{b}'$

Řešíme (5.3) s $\boldsymbol{b}' = \boldsymbol{0}$ postupně pro $n-r$ vektorů volných proměnných $\boldsymbol{t} = \boldsymbol{t}^{(i)}$, $i = 1, \dots, n-r$, kde $t_q^{(i)} = \delta_{i,q}$ (Kroneckerův symbol), neboli $t_i^{(i)} = 1$ a nula jinak. Rovnice (5.3) tak budou tvaru $\boldsymbol{U}\boldsymbol{y} = -\boldsymbol{U}'(:,i) = -\boldsymbol{S}'(:,k_i)$ a jejich řešením dostaneme $n-r$ odpovídajících vektorů $\boldsymbol{y}^{(i)}$ vázaných proměnných určujících $n-r$ řešení $\boldsymbol{u}^{(i)}$ homogenního systému $\boldsymbol{S}'\boldsymbol{u} = \boldsymbol{0}$ ze vztahů

$$u_j^{(i)} = \begin{cases} y_p^{(i)} & \text{jestliže } j = j_p \text{ pro nějaké } p \text{ a} \\ 1 & \text{jestliže } j = k_q \text{ pro } q = i \\ 0 & \text{jestliže } j = k_q \text{ pro nějaké } q \neq i. \end{cases}$$

Tento systém je nezávislý, neboť matice z nich vytvořená obsahuje jednotkovou submatici řádu $n-r$, která je regulární (viz 4.19(3)(4)). Protože je $\boldsymbol{u}^{(i)} \in \mathcal{N}(\boldsymbol{S}')$ a $\dim \mathcal{N}(\boldsymbol{S}') = n - \mathrm{r}(\boldsymbol{S}') = n-r$, musí tvořit jeho bázi (viz též 3.24(4)(ii)). Množina všech řešení je pak určena dle 5.3(2) následujícími vztahy, kde $t_1, \dots, t_{n-r} \in \mathbb{F}$ jsou libovolně zvolené volné proměnné:

$$\begin{array}{ccccccccc} x_1 & = & x_1^{(0)} & + & t_1.u_1^{(1)} & + & \cdots & + & t_{n-r}.u_1^{(n-r)} \\ x_2 & = & x_2^{(0)} & + & t_1.u_2^{(1)} & + & \cdots & + & t_{n-r}.u_2^{(n-r)} \\ \vdots & & \vdots & & \vdots & & \cdots & & \vdots \\ x_n & = & x_n^{(0)} & + & t_1.u_n^{(1)} & + & \cdots & + & t_{n-r}.u_n^{(n-r)} \end{array} \tag{5.4}$$

Poznámka: Pomocí systému MATLAB lze (dokonce ortonormální) bázi jádra $\mathcal{N}(\boldsymbol{A}) = \mathcal{N}(\boldsymbol{S}')$ snadno nalézt užitím příkazu `null`$(\boldsymbol{A})$.

(2) Jordanova eliminace

Postupujeme analogicky jako při Gaussově eliminaci (1) s tím rozdílem, že v kroku a) provádíme převod na schodovitý tvar pomocí Jordanovy metody popsané v poznámce 4.41(4). Při této metodě je v každém kroku eliminována i část sloupce nad každým schodem. Za cenu většího počtu výpočetních operací tak získáme jednodušší schodovitý tvar $\boldsymbol{S'}$, v němž regulární horní trojúhelníková submatice $\boldsymbol{U}$ se stane diagonální maticí, což výrazně zjednoduší výpočty v následných krocích c) a d). Rovnice (5.3) má diagonální matici soustavy, takže vázané proměnné partikulárního řešení určíme z rovnice $\boldsymbol{Uy} = \boldsymbol{b'}$ pouhým vydělením diagonálními prvky $u_{jj} \neq 0$: $y_j = \frac{b'_j}{u_{jj}}$ pro $j = 1, \ldots, r$. Stejně snadno určíme v kroku d) vázané proměnné bázových vektorů $\boldsymbol{u}_j^{(i)}$: $y_j^{(i)} = \frac{-U'(j,i)}{u_{jj}} = \frac{-S'(j,k_i)}{u_{jj}}$ pro $j = 1, \ldots, r$ a $i = 1, \ldots, n-r$.

(3) Užití LU-rozkladu

Nechť $\boldsymbol{PA} = \boldsymbol{LS}$ je LU-rozklad matice $\boldsymbol{A}$. Zřejmě platí:
$\boldsymbol{Ax} = \boldsymbol{b} \Leftrightarrow \boldsymbol{PAx} = \boldsymbol{Pb} \Leftrightarrow \boldsymbol{LSx} = \boldsymbol{Pb} \Leftrightarrow \boldsymbol{Lz} = \boldsymbol{Pb}$, kde $\boldsymbol{z} := \boldsymbol{Sx}$.
Celý postup hledání řešení tak sestává ze čtyř kroků:

a) Konstrukce matic $\boldsymbol{L}, \boldsymbol{U}$ a $\boldsymbol{P}$ podle 4.38

b) Provedení permutace pravé strany $\boldsymbol{Pb}$

c) Řešení soustavy $\boldsymbol{Lz} = \boldsymbol{Pb}$ algoritmem dopřed. dosazování (5.2a)

Matice $\boldsymbol{L}$ je dolní trojúhelníková a regulární, takže podle 5.3(1) existuje právě jedno řešení $\boldsymbol{z}$. Matice $\boldsymbol{L} =: [l_{ij}]$ má dokonce jednotkovou diagonálu, takže při dopředném dosazování nemusíme v rovnicích (5.2a) dělit diagonálními prvky $l_{ii} = 1$.

d) Řešení soustavy $\boldsymbol{Sx} = \boldsymbol{z}$ algoritmem zpětného dosazování (5.2b)

Rozhodneme o řešitelnosti a případně hledáme řešení stejně jako v krocích b) až d) Gaussovy eliminace (1). Pouze pravou stranu $\boldsymbol{b'}$ zaměníme vektorem $\boldsymbol{z}$.

5.7. Výpočetní složitost algoritmů (1) až (3).
Všechny algoritmy mají stejnou kubickou aditivní i multiplikativní složitost:

Aditivní složitost:

$$\mathcal{O}(\pm) = \boxed{\frac{n^3 - n}{3} + \frac{n^2 - n}{2}}$$

Multiplikativní složitost:

$$\mathcal{O}(*, /) = \boxed{\frac{n^3 - n}{3} + n^2}$$

Z hlediska výpočtové složitosti jsou všechny algoritmy ekvivalentní. Vzhledem k tomu, že ve všech třech metodách má nejvyšší výpočetní nároky triangularizace (převod na horní trojúhelníkový tvar: faktor $\frac{n^3-n}{3}$), resp. diagonalizace u Jordanovy metody, bude algoritmus (3) výhodnější v případě, že řešíme systém opakovaně s různými pravými stranami $\boldsymbol{b}$ a stejnou maticí soustavy $\boldsymbol{A}$. V takovém případě totiž stačí provést triangularizaci $\boldsymbol{PA} = \boldsymbol{LU}$ jen jednou, neboť nezávisí na pravé straně, a pak opakovaně provádět kroky b) až d) pro jednotlivé pravé strany. Tohoto postupu lze využít při řešení maticových rovnic typu $\boldsymbol{A}.\boldsymbol{X} = \boldsymbol{B}$, jehož speciálním případem je úloha nalezení inverze regulární čtvercové matice (viz dále odst. 5.5).

(4) Cramerovo pravidlo pro regulární čtvercovou matici soustavy $\boldsymbol{A}$.

Je-li $\boldsymbol{A}$ regulární čtvercová matice řádu n, pak $\boldsymbol{x} = \boldsymbol{A}^{-1}\boldsymbol{b}$ je zřejmě (jediné) hledané řešení soustavy $\boldsymbol{Ax} = \boldsymbol{b}$, neboť $\boldsymbol{AA}^{-1}\boldsymbol{b} = \boldsymbol{b}$ v důsledku rovnosti $\boldsymbol{AA}^{-1} = \boldsymbol{I}_n$. Toto řešení můžeme spočíst Cramerovým pravidlem 4.54. Metoda však vyžaduje spočtení $n+1$ determinantů řádu n a je proto použitelná jen pro soustavy o malém počtu rovnic ($n \leq 3$) a nebo ve speciálních případech, např. při vyjadřování řešení v symbolickém tvaru u rovnic, kde matice soustavy závisí na dalších parametrech. Pro numerické řešení větších soustav není vhodná také vzhledem k šíření numerických chyb při výpočtu (důsledek velkého počtu prováděných operací). Dochází tak ke ztrátě přesnosti, zejména v případech, kdy $\boldsymbol{A}$ se blíží k singulární matici ($\det \boldsymbol{A}$ je nepřesně spočtené malé číslo, kterým se při Cramerově pravidlu dělí). Takovým maticím říkáme **špatně podmíněné** (podrobněji viz dále odst. 5.6).

5.3. SLR s pásovou (tridiagonální) maticí soustavy.

Věta 5.8. *Nechť $\boldsymbol{Ax} = \boldsymbol{b}$, kde $\boldsymbol{A}$ je regulární pásová tridiagonální matice ($a_{ij} = 0$ pro $|i-j| > 1$) rozměru $n \times n$:*

$$\boldsymbol{A} = \begin{bmatrix} a_1 & c_1 & 0 & \dots & 0 & 0 & 0 \\ b_2 & a_2 & c_2 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & b_{n-1} & a_{n-1} & c_{n-1} \\ 0 & 0 & 0 & \dots & 0 & b_n & a_n \end{bmatrix}.$$

Potom její LU-rozklad $\boldsymbol{A} = \boldsymbol{LU}$ je tvaru

$$\boldsymbol{L} = \begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ \beta_2 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & \beta_n & 1 \end{bmatrix}, \boldsymbol{U} = \begin{bmatrix} \alpha_1 & c_1 & 0 & \dots & 0 \\ 0 & \alpha_2 & c_2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & c_{n-1} \\ 0 & 0 & 0 & \dots & \alpha_n \end{bmatrix},$$

kde $\alpha_1 = a_1$

$$\beta_i = \frac{b_i}{\alpha_{i-1}} \tag{5.5a}$$

$$\alpha_i = a_i - \beta_i c_{i-1} \quad \textit{pro } i = 2, 3, \dots, n.$$

Důkaz. Vztahy pro neznámé α_i a β_i snadno nalezneme formálním porovnáním prvků matic na levé a pravé straně po roznásobení maticové rovnice $\boldsymbol{A} = \boldsymbol{LU}$: viz též poznámku 5.9(3). □

Poznámka 5.9.

(1) Jinou variantu algoritmu (5.5a) lze odvodit pro

$$\boldsymbol{L} = \begin{bmatrix} \alpha_1 & 0 & \dots & 0 & 0 \\ b_2 & \alpha_2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & \alpha_{n-1} & 0 \\ 0 & 0 & \dots & b_n & \alpha_n \end{bmatrix}, \boldsymbol{U} = \begin{bmatrix} 1 & \gamma_1 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & \gamma_{n-1} \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix},$$

kde $\alpha_1 = a_1,\ \gamma_1 = \dfrac{c_1}{\alpha_1}$

$$\begin{aligned} \alpha_i &= a_i - b_i\gamma_{i-1} \\ \gamma_i &= \frac{c_i}{\alpha_i} \qquad \text{pro } i = 2, 3, \dots, n. \end{aligned} \tag{5.5b}$$

(2) Analogické algoritmy obdržíme pro blokově tridiagonální matice, kde $a_i, b_i, c_i, \alpha_i, \beta_i$ (resp. γ_i) jsou submatice kompatibilních rozměrů. Pak místo $\frac{1}{\alpha_{i-1}}$ násobíme inverzní maticí α_{i-1}^{-1} zprava v (5.5a) (resp. místo $\frac{1}{\alpha_i}$ maticí α_i^{-1} zleva v (5.5b)).

(3) V případě obecné regulární čtvercové matice $\boldsymbol{A}$ lze výše popsaný postup zobecnit pro přímý výpočet prvků matic $\boldsymbol{L}$ a $\boldsymbol{U}$ tak, že postupně sestavujeme rovnice pro prvky 1. řádku $\boldsymbol{U}$, 1. sloupce $\boldsymbol{L}$, 2. řádku $\boldsymbol{U}$, 2. sloupce $\boldsymbol{L}$, atd.

5.4. Přibližné řešení SLR metodou nejmenších čtverců.

Pokud neexistuje řešení SLR $\boldsymbol{Ax} = \boldsymbol{b}$, je to důsledkem toho, že $\boldsymbol{b} \notin \mathcal{R}(\boldsymbol{A})$. V tomto případě má smysl hledat řešení $\boldsymbol{x}$, které minimalizuje v nějakém smyslu chybu $\boldsymbol{b} - \boldsymbol{Ax}$. Chybu obvykle měříme vhodnou normou $\|\boldsymbol{b} - \boldsymbol{Ax}\|$. Nejčastěji se pro tento účel užívají p-normy (viz 3.56). Pokud je norma odvozena[24] z nějakého vnitřního součinu $\langle\cdot,\cdot\rangle$, stačí nahradit pravou stranu $\boldsymbol{b}$ její ortogonální projekcí $\widehat{\boldsymbol{b}} \in \mathcal{R}(\boldsymbol{A})$ na

[24] viz 3.62(S9).

$\mathcal{R}(\boldsymbol{A})$, což je dle věty o ortogonální projekci 3.77 vektor z $\mathcal{R}(\boldsymbol{A})$ minimalizující $\|\boldsymbol{b}-\widehat{\boldsymbol{b}}\|$. Místo původní rovnice pak řešíme rovnici $\boldsymbol{A}\boldsymbol{x}=\widehat{\boldsymbol{b}}$ tzv. **metodou nejmenších čtverců (MNČ)** podle následující věty.

<u>VĚTA</u> 5.10 (Metoda nejmenších čtverců ve $(V,\mathcal{L}_{\mathbb{F}})$)**.**
Nechť $(V,\mathcal{L}_{\mathbb{F}})$ je VS-prostor nad skalárním polem $\mathbb{F}\subseteq\mathbb{C}$ a $W:=\mathcal{L}(A)$ jeho vektorový podprostor generovaný konečnou množinou vektorů $A:=\{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_n\}$. Pak $\boldsymbol{\beta}=:[\beta_1,\ldots,\beta_n]\in\mathbb{F}^n$ je ve smyslu věty 3.77 řešením úlohy ortogonální projekce $P_W\boldsymbol{b}=:\widehat{\boldsymbol{b}}=\beta_1\boldsymbol{a}_1+\cdots+\beta_n\boldsymbol{a}_n$ vektoru $\boldsymbol{b}\in V$ na podprostor W právě když $\boldsymbol{\beta}$ je přesným řešením následujícího systému lineárních rovnic, který je vždy řešitelný:

$$\begin{array}{ccccccccc}
\langle\boldsymbol{a}_1,\boldsymbol{a}_1\rangle\beta_1 & + & \langle\boldsymbol{a}_2,\boldsymbol{a}_1\rangle\beta_2 & + & \ldots & + & \langle\boldsymbol{a}_n,\boldsymbol{a}_1\rangle\beta_n & = & \langle\boldsymbol{b},\boldsymbol{a}_1\rangle\\
\langle\boldsymbol{a}_1,\boldsymbol{a}_2\rangle\beta_1 & + & \langle\boldsymbol{a}_2,\boldsymbol{a}_2\rangle\beta_2 & + & \ldots & + & \langle\boldsymbol{a}_n,\boldsymbol{a}_2\rangle\beta_n & = & \langle\boldsymbol{b},\boldsymbol{a}_2\rangle\\
\vdots & & \vdots & & \ldots & & \vdots & & \vdots\\
\langle\boldsymbol{a}_1,\boldsymbol{a}_n\rangle\beta_1 & + & \langle\boldsymbol{a}_2,\boldsymbol{a}_n\rangle\beta_2 & + & \ldots & + & \langle\boldsymbol{a}_n,\boldsymbol{a}_n\rangle\beta_n & = & \langle\boldsymbol{b},\boldsymbol{a}_n\rangle.
\end{array}\tag{5.6a}$$

<u>DŮKAZ</u>. W je konečně rozměrný, takže podle 3.80 lze užít větu 3.77 o ortogonální projekci. Podle věty 3.86 je $P_W\boldsymbol{b}=\widehat{\boldsymbol{b}}\;\Leftrightarrow\;\boldsymbol{b}-\widehat{\boldsymbol{b}}\perp W \overset{3.72}{\Leftrightarrow} \boldsymbol{b}-\widehat{\boldsymbol{b}}\perp\boldsymbol{a}_i$ pro $i=1,\ldots,n \;\Leftrightarrow\; \langle\boldsymbol{b}-\sum_{j=1}^n\beta_j\boldsymbol{a}_j,\boldsymbol{a}_i\rangle=0$ pro $i=1,\ldots,n \overset{(3.1)}{\Leftrightarrow} \langle\boldsymbol{b},\boldsymbol{a}_i\rangle-\sum_{j=1}^n\beta_j\langle\boldsymbol{a}_j,\boldsymbol{a}_i\rangle=0$ pro $i=1,\ldots,n$ $\Leftrightarrow\sum_{j=1}^n\beta_j\langle\boldsymbol{a}_j,\boldsymbol{a}_i\rangle=\langle\boldsymbol{b},\boldsymbol{a}_i\rangle$ pro $i=1,\ldots,n\;\Leftrightarrow\boldsymbol{\beta}$ je řešením (5.6a). Řešitelnost tohoto systému je garantována větou o ortogonální projekci. $\square$

DŮSLEDEK 5.11 (Metoda nejmenších čtverců ve $(\mathbb{F}^m,\mathcal{L}_{\mathbb{F}})$)**.**
Nechť $\boldsymbol{A}=:[\boldsymbol{a}_1,\ldots,\boldsymbol{a}_n]$ je matice typu m/n tvořená sloupcovými vektory $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_n$ a $\boldsymbol{b}\in\mathbb{F}^m$ libovolný vektor. Pak $\boldsymbol{x}\in\mathbb{F}^n$ je řešením rovnice $\boldsymbol{A}\boldsymbol{x}=\widehat{\boldsymbol{b}}$ nad skalárním polem $\mathbb{F}\subseteq\mathbb{C}$ právě když $\boldsymbol{x}$ je přesným řešením následujícího systému lineárních rovnic:

$$(\boldsymbol{A}^*\boldsymbol{A})\boldsymbol{x}=\boldsymbol{A}^*\boldsymbol{b}.\tag{5.6b}$$

Tento systém je vždy řešitelný a jeho maticí soustavy je Gramova matice $\boldsymbol{A}^*\boldsymbol{A}$ — viz 4.14(9).

DŮKAZ. Jestliže nahradíme $\boldsymbol{\beta}$ v předchozí větě vektorem $\boldsymbol{x}$, pak $\widehat{\boldsymbol{b}} = x_1\boldsymbol{a}_1 + \cdots + x_n\boldsymbol{a}_n \overset{4.13}{=} \boldsymbol{A}\boldsymbol{x}$. Vektor $\boldsymbol{x}$ je tedy řešením této úlohy právě když je řešením SLR (5.6a), kde $\beta_i = x_i$. Tomuto systému odpovídá dle 4.14(9) maticový zápis (5.6b). Jeho řešitelnost je dána předchozí větou nebo také přímo plyne ihned z toho, že jeho pravá strana $\boldsymbol{A}^*\boldsymbol{b} \in \mathcal{R}(\boldsymbol{A}^*) \overset{3.88(5)(iii)}{=} \mathcal{R}(\boldsymbol{A}^*\boldsymbol{A})$. □

<u>*Poznámka*</u> 5.12.

(1) Jestliže $\mathbb{F} \subseteq \mathbb{R}$, pak v (5.6b) je $\boldsymbol{A}^* \overset{4.11(5)}{=} \boldsymbol{A}^T$.

(2) Je-li $\boldsymbol{W}$ nějaká pozitivně definitní matice řádu m (tzv. **váhová matice**), pak lze pomocí ní zavést v $\mathbb{F}^m$ *vážený skalární součin* $\langle \boldsymbol{x}, \boldsymbol{y}\rangle_{\boldsymbol{W}} := \langle \boldsymbol{W}\boldsymbol{x}, \boldsymbol{y}\rangle \overset{4.14(9)}{=} \boldsymbol{y}^*\boldsymbol{W}\boldsymbol{x}$ (podrobnosti dále v kapitole 6). Systém (5.6a) tak přejde v

$$(\boldsymbol{A}^*\boldsymbol{W}\boldsymbol{A})\boldsymbol{x} = \boldsymbol{A}^*\boldsymbol{W}\boldsymbol{b}. \tag{5.6c}$$

Jeho řešení nazýváme řešením úlohy $\boldsymbol{A}\boldsymbol{x} = \widehat{\boldsymbol{b}}$ tzv. **váženou metodu nejmenších čtverců s váhovou maticí $\boldsymbol{W}$**. Obvykle $\boldsymbol{W}$ je diagonální matice s kladnými diagonálními vahami $w_{ii} > 0$ (jinak $\boldsymbol{W}$ by totiž nebyla pozitivně definitní). Nechť $\boldsymbol{r} := \boldsymbol{b} - \boldsymbol{A}\boldsymbol{x}$ značí vektor odchylek řešení od pravé strany (tzv. **reziduální vektor**). Malá hodnota w_{ii} v odvozené normě $\|\boldsymbol{r}\|_{\boldsymbol{W}} = \sqrt{\langle \boldsymbol{W}\boldsymbol{r}, \boldsymbol{r}\rangle_{\boldsymbol{W}}} = \sqrt{\boldsymbol{r}^*\boldsymbol{W}\boldsymbol{r}} = \sqrt{\sum_{i=1}^m w_{ii} r_i \overline{r}_i} = \sqrt{\sum_{i=1}^m w_{ii}|r_i|^2}$ snižuje vliv odchylky r_i na hodnotu normy a připouští tudíž větší odchylku i-té složky oproti j-té složce, kde $w_{jj} > w_{ii}$.

(3) Je-li $\boldsymbol{b} \in \mathcal{R}(\boldsymbol{A})$, pak $\widehat{\boldsymbol{b}} = P_W\boldsymbol{b} \overset{3.76(1)}{=} \boldsymbol{b}$, takže každé řešení soustavy (5.6b) je současně přesným řešením původní rovnice $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}$. V MATLABu pro nečtvercovou matici pomocí operátoru levého dělení $\boldsymbol{x} = \boldsymbol{A}\backslash\boldsymbol{b}$ spočteme nějaké (partikulární)

MNČ-řešení systému (5.6b). Toto řešení je přesné, pokud je původní systém řešitelný — viz poznámku v 5.2(1)c).

5.5. Řešení maticové rovnice $\boldsymbol{A}.\boldsymbol{X} = \boldsymbol{B}$ a výpočet inverze $\boldsymbol{A}^{-1}$.

Nechť $\boldsymbol{A}$ typu m/n a $\boldsymbol{B}$ typu m/p jsou dané matice. Řešením maticové rovnice $\boldsymbol{A}.\boldsymbol{X} = \boldsymbol{B}$ rozumíme každou matici $\boldsymbol{X}$ kompatibilního typu n/p, která tuto rovnici splňuje. Protože $\boldsymbol{A}.\boldsymbol{X} = \boldsymbol{B} \Leftrightarrow \boldsymbol{A}.X(:,k) = B(:,k)$ pro $k = 1,\ldots,p$, vidíme, že sloupce $\boldsymbol{X}$ jsou po řadě řešení p systémů lineárních rovnic s pravými stranami tvořenými odpovídajícími sloupci matice $\boldsymbol{B}$. Všechny tyto systémy mají přitom stejnou maticí soustavy $\boldsymbol{A}$.
V zásadě můžeme po drobné modifikaci užít metody (1) až (3) z odst. 5.2.

(1) Gaussova nebo Jordanova eliminace
V kroku a) převádíme na schodovitý tvar matici soustavy rozšířenou o všechny pravé strany, tj. matici $\widetilde{\boldsymbol{A}} = [\boldsymbol{A}, \boldsymbol{B}]$. Obdržíme $[\boldsymbol{S}, \boldsymbol{B}']$.
V kroku b) rozhodnutí o řešitelnosti maticové rovnice spočívá v rozhodnutí o řešitelnosti všech ekvivalentních soustav s měnícími se pravými stranami $B'(:,k)$, $k = 1,\ldots,p$. Snadno nahlédneme, že nutnou a postačující podmínkou je opět podmínka $\mathrm{r}(\boldsymbol{A}) = \mathrm{r}(\widetilde{\boldsymbol{A}})$, tj. stejný počet nenulových řádků v maticích $\boldsymbol{S}$ a $[\boldsymbol{S}, \boldsymbol{B}']$.
V kroku c) pak (5.3) řešíme postupně s pravými stranami $\boldsymbol{b}' = B'(:,k)$ pro $k = 1,\ldots,p$. Krok d) zůstane beze změny, neboť nezávisí na pravé straně.

(2) Užití LU-rozkladu
Jak již bylo zmíněno v 5.7, stačí vlastní LU-rozklad z kroku a) provést pouze jednou, v kroku b) pak provedeme řádkovou permutaci $\boldsymbol{PB}$ celé matice $\boldsymbol{B}$, což odpovídá řádkovým permutacím všech pravých stran. Nakonec pro každou pravou stranu (sloupce matice $\boldsymbol{B}$) opakujeme kroky c)d), čímž postupně dostáváme jako řešení odpovídající sloupce neznámé matice $\boldsymbol{X}$.

Analogicky jako v odst. 5.4 lze přibližné MNČ-řešení maticové rovnice $\boldsymbol{A}.\boldsymbol{X} = \boldsymbol{B}$ nalézt řešením maticové rovnice $(\boldsymbol{A}^*\boldsymbol{A})\boldsymbol{X} = \boldsymbol{A}^*\boldsymbol{B}$, která je vždy řešitelná.

Je-li $\boldsymbol{A}$ regulární čtvercová matice řádu n, pak k nalezení inverze $\boldsymbol{X} = \boldsymbol{A}^{-1}$ stačí podle 4.46(11) řešit maticovou rovnici $\boldsymbol{A}.\boldsymbol{X} = \boldsymbol{I}_n$. Tato úloha je tak speciálním případem maticové rovnice $(m = n = p)$. Poznamenejme ještě, že v případě regulární matice, je $\boldsymbol{A}^{-1}\boldsymbol{B}$ (jediným) řešením obecné maticové rovnice s libovolnou pravou stranou $\boldsymbol{B}$. V případě regulární matice $\boldsymbol{A}$ nízkého řádu, můžeme pro výpočet její inverze užít také determinantovou metodu dle důsledku 4.53.

5.6. Problémy s numerickou nestabilitou při řešení SLR.

Matice $\boldsymbol{A}$ se nazývá **špatně podmíněná**, jestliže malé změny pravé strany $\boldsymbol{b}$ mají za následek velké změny řešení $\boldsymbol{x}$. Například pro čtvercovou matici $\boldsymbol{A}$ tato situace nastává v případech, kdy $\boldsymbol{A}$ je sice regulární, avšak s malou hodnotou determinantu, neboli říkáme, že je "skoro singulární". Tato situace nastane, když některý sloupcový (řádkový) vektor v $\boldsymbol{A}$ svírá malý úhel s nadrovinou generovanou ostatními sloupci (řádky).
Jako příklad uvažme následující systém dvou lineárních rovnic:

$$\begin{aligned} x + 2y &= 2 \\ 2x + 3y &= 3,4 \end{aligned}$$

Přesné řešení $x = 0,8$, $y = 0,6$ aproximujme dosti nepřesně hodnotami $\widetilde{x} = 1$, $\widetilde{y} = 0,48$. Po jejich dosazení do obou rovnic dostáváme po řadě $1,96$ místo 2 a $3,44$ místo $3,4$, což jsou malé odchylky řádově v setinách ve srovnání s chybou řešení, která je řádově v desetinách. Příčina tkví v tom, že hledáme průsečík dvou přímek, které svírají velmi malý úhel o směrnicích $-\frac{1}{2}$ a $-\frac{2}{3}$. Řádky $[1,2]$ a $[2,3]$ matice soustavy v tomto případě totiž reprezentují souřadnice kolmic k oběma přímkám a svírají tedy stejný úhel jako přímky samotné.

Se zmenšujícím se úhlem se blížíme ke stavu lineární závislosti obou vektorů, tj. ke stavu, kdy matice soustavy je singulární.
Podobně lze zkonstruovat situace, kdy při libovolně velké odchylce řešení lze dosáhnout libovolně malé odchylky od pravé strany.

ZÁVĚR: *Nelze tedy hodnotit přesnost nalezeného řešení podle odchylek od pravé strany po jeho dosazení do rovnic!*

Lze pouze hodnotit podmíněnost matice. Ta se měří číslem podmíněnosti, které se zpravidla počítá jako poměr největšího ku nejmenšímu singulárnímu číslu matice. Singulární čísla matice $\boldsymbol{A}$ jsou druhé odmocniny vlastních čísel symetrické matice $\boldsymbol{A}^T\boldsymbol{A}$ — tedy v případě symetrické matice splývají s jejími vlastními čísly (podrobněji viz následující kapitolu). Toto číslo podmíněnosti v systému MATLAB počítá funkce `cond`. Čím větší číslo podmíněnosti má daná matice, tím je hůře podmíněná a více se blíží k singulární matici. Jinak počítané reciproké číslo podmíněnosti v intervalu $[0,1]$ vrací funkce `rcond`. V tomto případě špatnou podmíněnost indikují hodnoty blízké k nule.

5.7. Iterační metody pro řešení systému lineárních rovnic.

Princip:
Rovnici $\boldsymbol{Ax}=\boldsymbol{b}$, kde $\boldsymbol{A}$ je čtvercová regulární matice řádu n, převedeme na rovnici tvaru $\boldsymbol{x}=\boldsymbol{\Gamma x}+\boldsymbol{\gamma}$, kterou generujeme posloupnost iterací.

Obecný postup hledání $\boldsymbol{\Gamma}$ a $\boldsymbol{\gamma}$:
Matici $\boldsymbol{A}$ vhodně rozložíme do tvaru $\boldsymbol{A}=\boldsymbol{N}-\boldsymbol{M}$, kde $\boldsymbol{N}$ je regulární matice. Pak platí

$$\boldsymbol{Ax}=\boldsymbol{b} \quad\Leftrightarrow\quad (\boldsymbol{N}-\boldsymbol{M})\boldsymbol{x}=\boldsymbol{b} \quad\Leftrightarrow\quad \boldsymbol{Nx}=\boldsymbol{Mx}+\boldsymbol{b} \quad\Leftrightarrow$$
$$\boldsymbol{x}=\underbrace{\boldsymbol{N}^{-1}\boldsymbol{M}}_{\boldsymbol{\Gamma}}\boldsymbol{x}+\underbrace{\boldsymbol{N}^{-1}\boldsymbol{b}}_{\boldsymbol{\gamma}}.$$

Iterační proces:

$$\boxed{\begin{array}{lcl} \boldsymbol{x}^{(0)} & \dots & \text{počáteční iterace} \\ \boldsymbol{x}^{(k+1)} & = & \boldsymbol{\Gamma}\boldsymbol{x}^{(k)} + \boldsymbol{\gamma} \quad \text{pro } k = 0, 1, \dots . \end{array}} \tag{5.7}$$

DEFINICE 5.13 (Jacobiho prosté iterace)**.**
Položíme

$$\boldsymbol{N} := \operatorname{diag}(\boldsymbol{A}) = \begin{bmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{nn} \end{bmatrix}$$

$$\boldsymbol{M} := \boldsymbol{N} - \boldsymbol{A} = \begin{bmatrix} 0 & -a_{12} & \dots & -a_{1n} \\ -a_{21} & 0 & \dots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \dots & 0 \end{bmatrix},$$

pak

$$\boldsymbol{\Gamma} = \begin{bmatrix} 0 & -\frac{a_{12}}{a_{11}} & \dots & -\frac{a_{1n}}{a_{11}} \\ -\frac{a_{21}}{a_{22}} & 0 & \dots & -\frac{a_{2n}}{a_{22}} \\ \vdots & \vdots & \ddots & \vdots \\ -\frac{a_{n1}}{a_{nn}} & -\frac{a_{n2}}{a_{nn}} & \dots & 0 \end{bmatrix}, \quad \boldsymbol{\gamma} = \begin{bmatrix} \frac{b_1}{a_{11}} \\ \frac{b_2}{a_{22}} \\ \vdots \\ \frac{b_n}{a_{nn}} \end{bmatrix}.$$

Rozepsáním (5.7) do jednotlivých rovnic dostáváme
Jacobiho iterační proces:

$$\boxed{\begin{array}{rcl} x_1^{(0)}, \dots, x_n^{(0)} & \dots & \text{počáteční iterace} \\ x_j^{(k+1)} & = & \frac{1}{a_{jj}}\big(b_j - \sum_{\substack{i=1 \\ i \neq j}}^{n} a_{ji}\, x_i^{(k)}\big), \\ j & = & 1, \dots, n; \; k = 0, 1, \dots . \end{array}} \tag{5.8}$$

Vidíme, že vztah pro $x_j^{(k+1)}$ odpovídá formálnímu vyřešení j-té rovnice vzhledem k proměnné x_j.

Jestliže nyní v (5.8) použijeme pro $i < j$ již spočtenou iteraci $x_i^{(k+1)}$ místo $x_i^{(k)}$, obdržíme následující zřejmě poněkud rychleji konvergující iterační proces.

DEFINICE 5.14 (Gauss-Seidelovy iterace)**.**
Položíme

$$\boldsymbol{N} := \begin{bmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix},$$

$$\boldsymbol{M} := \boldsymbol{N} - \boldsymbol{A} = \begin{bmatrix} 0 & -a_{12} & \dots & -a_{1n} \\ 0 & 0 & \dots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix},$$

pak z $\boldsymbol{N}\boldsymbol{x}^{(k+1)} = \boldsymbol{M}\boldsymbol{x}^{(k)} + \boldsymbol{b}$ dostáváme ihned rovnice pro

Gauss-Seidelův iterační proces:

$$\boxed{\begin{array}{rcl} x_1^{(0)}, \dots, x_n^{(0)} & \dots & \text{počáteční iterace} \\ x_j^{(k+1)} & = & \frac{1}{a_{jj}}\left(b_j - \sum_{i=1}^{j-1} a_{ji}\, x_i^{(k+1)} - \sum_{i=j+1}^{n} a_{ji}\, x_i^{(k)}\right), \\ j & = & 1, \dots, n;\ k = 0, 1, \dots . \end{array}} \tag{5.9}$$

DEFINICE 5.15. Čtvercová matice $\boldsymbol{A}$ řádu n se nazývá **striktně diagonálně dominantní**, jestliže $|a_{jj}| > \sum_{\substack{i=1 \\ i \neq j}}^{n} |a_{ji}|$ pro $j = 1, 2, \dots, n$.

VĚTA 5.16 (Konvergence Jacobiho a Gauss-Seidelovy metody)**.**
Nechť $\boldsymbol{A}$ je striktně diagonálně dominantní matice. Potom systém lineárních rovnic $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}$ má jediné řešení a Jacobiho i Gauss-Seidelův

iterační proces konverguje k tomuto řešení při libovolně zvolené počáteční aproximaci $\boldsymbol{x}^{(0)}$.

<u>*POZNÁMKA*</u> 5.17. Obecně z konvergence jedné z obou metod neplyne konvergence druhé. Pokud konvergují obě, pak Gauss-Seidelova metoda konverguje rychleji.

PŘÍKLAD 5.18. Jak ukazuje následující příklad, může pouhou změnou pořadí rovnic dojít ke ztrátě konvergence. Uvažme SLR

$$\begin{array}{rcrcrcr} 4x & - & y & + & z & = & 7 \\ 4x & - & 8y & + & z & = & -21 \\ -2x & + & y & + & 5z & = & 15 \end{array}$$

Jacobiho iterace tohoto SLR odstartované v počáteční aproximaci $\boldsymbol{x}^{(0)} = [1, 2, 2]$ konvergují k přesnému řešení $\boldsymbol{x} = [2, 4, 3]$, neboť matice soustavy je striktně diagonálně dominantní.

Jestliže zaměníme první a poslední rovnici, tak se tato vlastnost poruší a SLR

$$\begin{array}{rcrcrcr} -2x & + & y & + & 5z & = & 15 \\ 4x & - & 8y & + & z & = & -21 \\ 4x & - & y & + & z & = & 7 \end{array}$$

při téže počáteční iteraci diverguje od přesného řešení.

<u>*Poznámka*</u> 5.19. Iterační metody jsou vhodné zejména pro rozsáhlé systémy lineárních rovnic s řídkou maticí soustavy (malým počtem nenulových prvků), kde u Gaussovy eliminace bývají problémy s numerickou stabilitou (viz 5.6) a větší výpočetní nároky vzhledem k nemožnosti účelně využít případné řídkosti matice soustavy.
Snažíme se vhodnou záměnou pořadí rovnic (řádkovou permutací rozšířené matice soustavy) a změnou pořadí nezávisle proměnných (sloupcová permutace matice soustavy) soustředit největší nenulové prvky kolem hlavní diagonály s cílem dosáhnout (pokud možno) striktně diagonální dominantnosti. To je zpravidla snazší u řídké matice, která se stane pásovou (nenulové prvky soustředěny kolem hlavní diagonály).

ANGLICKÁ TERMINOLOGIE PRO LINEÁRNÍ ROVNICE

systém lineárních rovnic (SLR) ♦ system of linear equations (SLE)
matice systému ♦ matrix of the system
pravá strana ♦ right-hand side
vektor neznámých ♦ vector of unknowns
(ne)homogenní systém ♦ (non-)homogeneous system
rozšířená matice SLR ♦ augmented matrix of a SLE
množina řešení ♦ solution set
partikulární řešení ♦ particular solution
algoritmus dopředného dosazování ♦ forward-substitution algorithm
algoritmus zpětného dosazování ♦ back-substitution algorithm
SLR s dolní trojúhelníkovou maticí ♦ lower-triangular SLE
SLR s horní trojúhelníkovou maticí ♦ upper-triangular SLE
výpočetní složitost ♦ computational complexity
tridiagonální matice ♦ tridiagonal matrix
pásová matice ♦ band matrix
přibližné řešení ♦ approximate solution
metoda nejmenších čtverců (MNČ) ♦ least-squares (LSQ) solution
vážená MNČ ♦ weighted LSQ method
váhová matice ♦ weight matrix
maticová rovnice ♦ matrix equation
numerická (ne)stabilita ♦ numerical (in)stability
špatně podmíněná matice ♦ badly-conditioned matrix
dobře podmíněná matice ♦ well-conditioned matrix
číslo podmíněnosti ♦ condition number
iterační metoda ♦ iterative method

6. Transformace souřadnic a diagonalizace matic

Látka je předběžně zpracována v souborech `TrSour.tif` a `DiagMat.tif`, které jsou zkomprimovány v `TrSour.zip` a v `DiagMat.zip`.

Nechť dále značí $a := a_1 + ia_2, b := b_1 + ib_2$ dvě komplexní čísla v kartézském tvaru a
$a = |a|(\cos\alpha + i\sin\alpha) = |a|e^{i\alpha}$, $b = |b|(\cos\beta + i\sin\beta) = |b|e^{i\beta}$ jejich vyjádření v goniometrickém, resp. Eulerově tvaru.
Jelikož funkce kosinus je sudá ($\cos(-x) = \cos(x)$) a funkce sinus lichá ($\sin(-x) = -\sin(x)$), dostáváme:

$$\overline{e^{i\alpha}} = e^{-i\alpha} \text{ a tedy } \overline{a} = |a|e^{-i\alpha} \text{ a } \overline{b} = |b|e^{-i\beta}.$$

A.1. **Sečítání, odčítání.**

$$a + b := (a_1 + b_1) + i(a_2 + b_2)$$
$$a - b := (a_1 - b_1) + i(a_2 - b_2)$$

A.2. **Násobení.**

$$ab = (a_1 + ia_2)(b_1 + ib_2) = (a_1b_1 - a_2b_2) + i(a_2b_1 + a_1b_2) \quad \text{nebo}$$
$$ab = |a|e^{i\alpha}|b|e^{i\beta} = |a||b|e^{i(\alpha+\beta)} = |a||b|(\cos(\alpha + \beta) + i\sin(\alpha + \beta)).$$

Zejména platí

$$a\overline{a} = a_1^2 + a_2^2 = |a|^2.$$

A.3. **Dělení.** Nechť $b \neq 0$, pak

$$\frac{a}{b} = \frac{a\overline{b}}{b\overline{b}} = \frac{a_1b_1 + a_2b_2}{b_1^2 + b_2^2} + i\frac{a_2b_1 - a_1b_2}{b_1^2 + b_2^2} \quad \text{nebo}$$
$$\frac{a}{b} = \frac{|a|e^{i\alpha}}{|b|e^{i\beta}} = \frac{|a|}{|b|}e^{i(\alpha-\beta)} = \frac{|a|}{|b|}(\cos(\alpha - \beta) + i\sin(\alpha - \beta)).$$

A.4. **Umocňování.**

Tvrzení (Moivreova věta).

$$a^n = |a|^n(\cos\alpha n + i\sin\alpha n), \text{ kde } n \in \mathbb{Z}$$

Důkaz. Indukcí vzhledem k $|n|$ užitím vztahu A.2 pro násobení při $n > 0$, resp. vztahu A.3 pro dělení komplexních čísel při $n < 0$. □

A.5. **Odmocňování.**

1. Druhá odmocnina v kartézských souřadnicích

$$\sqrt{a_1 + ia_2} = \pm(u_1 + iu_2), \text{ kde}$$
$$u_1 = \sqrt{\frac{1}{2}(|a| + a_1)}$$
$$u_2 = \operatorname{sgn}(a_2)\sqrt{\frac{1}{2}(|a| - a_1)}, \text{ kde } \operatorname{sgn}(a_2) \text{ udává znaménko } a_2.$$

2. n-tá odmocnina

Uvažme, že vzhledem k periodicitě funkcí kosinus a sinus platí
$a = |a|(\cos\alpha + i\sin\alpha) = |a|(\cos(\alpha+2\pi k)+i\sin(\alpha+2\pi k)) = |a|e^{i(\alpha+2\pi k)}$
pro každé $k \in \mathbb{Z}$.
Odtud dostaneme ihned vztah pro všechny n-té odmocniny z a:

$$\sqrt[n]{a} = \sqrt[n]{|a|}e^{i\frac{\alpha+2\pi k}{n}} = \sqrt[n]{|a|}\left(\cos\frac{\alpha+2\pi k}{n} + i\sin\frac{\alpha+2\pi k}{n}\right)$$

pro $k = 0, 1, \ldots, n-1$.

3. n-tá odmocnina z 1

Z předchozího dostaneme volbou $a = 1$ všechny n-té odmocniny z 1:

$$\sqrt[n]{1} = e^{i\frac{2\pi k}{n}} = \left(\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}\right)$$

pro $k = 0, 1, \ldots, n-1$.

Tvrzení (Vlastnosti).

(1) Všechny hodnoty n-té odmocniny z komplexního čísla a dostaneme vynásobením jedné z těchto hodnot všemi hodnotami n-té odmocniny z 1.
(2) Jsou-li $\varepsilon_1, \varepsilon_2$ n-té odmocniny z 1, pak $\varepsilon_1\varepsilon_2$ je rovněž n-tá odmocnina z 1.
(3) Je-li ε k-tá odmocnina z 1 a $l = kq$, pak ε je rovněž l-tá odmocnina z 1.

(4) Je-li ε n-tá odmocnina z 1, pak $\varepsilon_k := \varepsilon^k$ je rovněž n-tá odmocnina z 1 pro $k = 0, 1, \dots, n-1$.
(5) ε se nazývá **primitivní** n-tá odmocnina z 1, platí-li:
(i) $\varepsilon^n = 1$
(ii) $\varepsilon^k \neq 1$ pro $k = 1, 2, \dots, n-1$.
(6) Je-li ε n-tá odmocnina z 1, pak ε je primitivní právě když hodnoty ε^k jsou pro $k = 0, 1, \dots, n-1$ navzájem různé. Zejména $\varepsilon := e^{\frac{i2\pi}{n}}$ je vždy primitivní, neboť $\varepsilon^k = e^{\frac{i2\pi k}{n}}$ jsou pro $k = 0, 1, \dots, n-1$ navzájem různá komplexní čísla.
(7) Nechť ε je primitivní n-tá odmocnina z 1. Pak ε^k je primitivní n-tá odmocnina z 1 právě když n a k jsou nesoudělné.
(8) Nechť p je prvočíslo, pak všechny p-té odmocniny z 1 různé od 1 jsou primitivní.

A.6. **Goniometrické vzorce.**

1. Vyjádření goniometrických funkcí $\sin n\alpha, \cos n\alpha$ pomocí $\sin\alpha, \cos\alpha$

Použitím Moivreovy věty a binomické věty dostáváme:

$$\cos n\alpha + i\sin n\alpha = (\cos\alpha + i\sin\alpha)^n = \\ = \sum_{k=0}^{n} \binom{n}{k} \cos^k\alpha\ (i)^{n-k} \sin^{n-k}\alpha.$$

Stačí pak porovnat reálné, popřípadě imaginární části výrazů vlevo a vpravo. Zejména pro $n = 2$ tak dostáváme známé vztahy pro dvojnásobný úhel:

$$\cos 2\alpha = \cos^2\alpha - \sin^2\alpha,\ \sin 2\alpha = 2\sin\alpha\cos\alpha.$$

Ty jsou však speciálním případem obecnějších vztahů pro součet a rozdíl úhlů, získaných z A.2 volbou $a_1 = \cos\alpha, a_2 = \sin\alpha$ a $b_1 = \cos(\pm\beta) = \cos\beta, b_2 = \sin(\pm\beta) = \pm\sin\beta$. Jelikož $|a| = |b| = 1$, obdržíme:

$$\cos(\alpha \pm \beta) = \cos\alpha\cos\beta \mp \sin\alpha\sin\beta,$$
$$\sin(\alpha \pm \beta) = \sin\alpha\cos\beta \pm \cos\alpha\sin\beta.$$

2. Vyjádření goniometrických funkcí $\sin^n \alpha, \cos^n \alpha$ pomocí $\sin k\alpha, \cos k\alpha$

Z Eulerova vztahu dostáváme vyjádření pro $\sin\alpha$ a $\cos\alpha$:

$$\sin\alpha = \frac{e^{i\alpha} - e^{-i\alpha}}{2i}, \ \cos\alpha = \frac{e^{i\alpha} + e^{-i\alpha}}{2}.$$

Ty stačí umocnit na n-tou opět užitím binomické věty:

$$\sin^n \alpha = \frac{1}{2^n i^n} \sum_{k=0}^{n} \binom{n}{k} e^{ik\alpha} \ (-1)^{n-k} e^{-i(n-k)\alpha}$$

$$\cos^n \alpha = \frac{1}{2^n} \sum_{k=0}^{n} \binom{n}{k} e^{ik\alpha} \ e^{-i(n-k)\alpha}.$$

Například spočtěme

$$\sin^3 \alpha = \frac{1}{2^3 i^3}(e^{i3\alpha} - 3e^{i2\alpha}e^{-i\alpha} + 3e^{i\alpha}e^{-i2\alpha} - e^{-i3\alpha}) =$$

$$= \frac{1}{8i^3}(2i\sin 3\alpha - 3.2i\sin\alpha) = \frac{1}{4i^2}(\sin 3\alpha - 3\sin\alpha) =$$

$$= \frac{1}{4}(3\sin\alpha - \sin 3\alpha).$$

Věta B.1. *Nechť $(V_1, \mathcal{L}_{\mathbb{F}})$, $(V_2, \mathcal{L}_{\mathbb{F}})$ a $(V_3, \mathcal{L}_{\mathbb{F}})$ jsou tři vektorové prostory konečných dimenzí $\dim V_1 = n$, $\dim V_2 = m$ a $\dim V_3 = p$. Pak zobrazení $T \mapsto [T]$ $(T \in \mathcal{L}(V_1, V_2))$ je izomorfizmem vektorového prostoru $\mathcal{L}(V_1, V_2)$ všech lineárních operátorů z V_1 do V_2 (viz 3.38) na vektorový prostor všech matic $\mathcal{M}_{m,n}$ (viz 4.9). Přitom platí:*

(1) $[T\boldsymbol{x}] = [T].[\boldsymbol{x}]$ *pro každé* $\boldsymbol{x} \in V_1$.

(2) *Složení dvou operátorů $T : V_1 \to V_2$ a $U : V_2 \to V_3$ odpovídá v souřadnicovém vyjádření součin matic: $[UT] = [U].[T]$.*

(3) *Maticovou reprezentací identického operátoru $I : V_1 \to V_1$ je jednotková matice: $[I] = \boldsymbol{I}_n$.*

(4) *Operátor T je surjektivní právě když je reprezentován maticí řádkově plné hodnosti*[25].

(5) *Operátor T je izomorfní vnoření právě když je reprezentován maticí sloupcově plné hodnosti*[25].

(6) *Operátor T je izomorfizmus právě když je reprezentován regulární maticí*[25]. *Přitom platí $[T]^{-1} = [T^{-1}]$, kde $[T]^{-1}$ je matice inverzní*[26] *k $[T]$.*

V případě VS-prostorů ($\mathbb{F} \subseteq \mathbb{C}$) navíc platí:

(7) *Maticovou reprezentací operátoru adjungovaného k T je hermitovsky transponovaná matice: $[T^*] = [T]^*$. Zejména maticovou reprezentaci samoadjungovaného operátoru je hermitovsky symetrická matice.*

(8) *Operátor T je unitární právě když je reprezentován unitární maticí.*

Důkaz. Nadále $E = \{\boldsymbol{e}_1, \dots, \boldsymbol{e}_1\}$ je nějaká pevně zvolená báze ve V_1.

• Linearita zobrazení $T \mapsto [T]$:

$[T_1 + T_2] = [[(T_1 + T_2)\boldsymbol{e}_1], \dots, [(T_1 + T_2)\boldsymbol{e}_n]] =$

---

[25] Viz definici 4.17.

[26] Matice určující maticový operátor inverzní k operátoru určenému maticí $[T]$ dle věty 4.25.

$[[T_1\boldsymbol{e}_1 + T_2\boldsymbol{e}_1], \dots, [T_1\boldsymbol{e}_n + T_2\boldsymbol{e}_n]] \overset{3.92}{=}$
$[[T_1\boldsymbol{e}_1] + [T_2\boldsymbol{e}_1], \dots, [T_1\boldsymbol{e}_n] + [T_2\boldsymbol{e}_n]] =$
$[[T_1\boldsymbol{e}_1], \dots, [T_1\boldsymbol{e}_n]] + [[T_2\boldsymbol{e}_1], \dots, [T_2\boldsymbol{e}_n]] = [T_1] + [T_2]$.
$[\alpha T] = [[(\alpha T)\boldsymbol{e}_1], \dots, [(\alpha T)\boldsymbol{e}_n]] = [[\alpha(T\boldsymbol{e}_1)], \dots, [\alpha(T\boldsymbol{e}_n)]] \overset{3.92}{=}$
$[\alpha[T\boldsymbol{e}_1], \dots, \alpha[T\boldsymbol{e}_n]] = \alpha[[T\boldsymbol{e}_1], \dots, [T\boldsymbol{e}_n]] = \alpha[T]$.

• $T \mapsto [T]$ je prosté:

$T_1 \neq T_2 \overset{3.35}{\Rightarrow} \exists i : T_1\boldsymbol{e}_i \neq T_2\boldsymbol{e}_i \overset{3.92}{\Rightarrow} \exists i : [T_1\boldsymbol{e}_i] \neq [T_2\boldsymbol{e}_i] \Rightarrow$ $[[T_1\boldsymbol{e}_1], \dots, [T_1\boldsymbol{e}_n]] \neq [[T_2\boldsymbol{e}_1], \dots, [T_2\boldsymbol{e}_n]] \Rightarrow [T_1] \neq [T_2]$.

• $T \mapsto [T]$ je surjekce:

Buď $\boldsymbol{A}$ libovolná matice typu m/n. Dle 3.92 je $[\cdot]$ surjekce, takže ke každému sloupci $A(:,j)$ existuje vektor $\boldsymbol{v}_j \in V_2$ tak, že $[\boldsymbol{v}_j] = A(:,j)$. Podle 3.36(6) lze zobrazení $\boldsymbol{e}_j \mapsto \boldsymbol{v}_j$ rozšířit na lineární operátor $V_1 \to V_2$, takže $[T\boldsymbol{e}_j] = [\boldsymbol{v}_j] = A(:,j) \Rightarrow [T] = [[T\boldsymbol{e}_1], \dots, [T\boldsymbol{e}_n]] = [A(:,1), \dots, A(:,n)] = \boldsymbol{A}$.

• Vlastnost (1):

Nechť $\boldsymbol{x} = \sum_{i=1}^n \xi_i \boldsymbol{e}_i$, tj. $\boldsymbol{\xi} = [\boldsymbol{x}]$. Pak $[T\boldsymbol{x}] = [T(\sum_{i=1}^n \xi_i \boldsymbol{e}_i)] = [\sum_{i=1}^n \xi_i T\boldsymbol{e}_i] \overset{3.92}{=} \sum_{i=1}^n \xi_i [T\boldsymbol{e}_i] \overset{4.13a)}{=} [[T\boldsymbol{e}_1], \dots, [T\boldsymbol{e}_n]].\boldsymbol{\xi} = [T].[\boldsymbol{x}]$.

• Vlastnost (2):

$[UT] = [[U(T\boldsymbol{e}_1)], \dots, [U(T\boldsymbol{e}_n)]] \overset{(1)}{=} [[U].[T\boldsymbol{e}_1], \dots, [U].[T\boldsymbol{e}_n]] \overset{4.15(1)}{=}$ $[U].[[T\boldsymbol{e}_1], \dots, [U].[T\boldsymbol{e}_n]] = [U].[T]$.

• Vlastnost (3):

$[I] = [[I\boldsymbol{e}_1], \dots, [I\boldsymbol{e}_n]] = [[\boldsymbol{e}_1], \dots, [\boldsymbol{e}_n]] = [\boldsymbol{\varepsilon}_1, \dots, \boldsymbol{\varepsilon}_n] = \boldsymbol{I}_n$.

• Vlastnosti (4)–(6),(8):

Označíme-li $S_1 : V_1 \to \mathbb{F}^n$ a $S_2 : V_2 \to \mathbb{F}^m$ unitární izomorfizmy přiřazení souřadnic (S_i zastupije zápis $[\cdot]$ ve 3.92), pak $[T\boldsymbol{x}] \overset{(1)}{=} [T].[\boldsymbol{x}]$ lze psát ve tvaru $S_2T\boldsymbol{x} = [T].(S_1\boldsymbol{x}) \overset{4.15}{=} [T]S_1\boldsymbol{x}$ pro každé $x \in \mathbb{F}^n$, což je ekvivalentní s rovností složených operátorů $S_2T = [T]S_1$. Aplikujeme-li na tuto rovnost S_2^{-1} zleva, resp. S_1^{-1} zprava, obdržíme vyjádření: $T = S_2^{-1}[T]S_1$, resp. $[T] = S_2TS_1^{-1}$. Složení tří izomorfních vnoření (surjekcí, izomorfizmů) je zřejmě opět izomorfní vnoření (surjekce, izomorfizmus). Jelikož S_1 i S_2 jsou izomorfizmy (surjektivní

izomorfní vnoření), z výše uvedených vyjádření T a $[T]$ vidíme, že T je izomorfní vnoření (surjekce, izomorfizmus) $\Leftrightarrow$ $[T]$ určuje izomorfní vnoření (surjekci, izomorfizmus), což je podle věty 4.20 ekvivalentní s dokazovanými tvrzeními o matici $[T]$. Protože S_i jsou unitární izomorfizmy a také složení tří unitárních izomorfizmů je rovněž unitární izomorfizmus, dostáváme podobně ekvivalenci s unitaritou maticového operátoru $[T]$ a tedy i s maticí $[T]$ (viz 4.15(8)).
T izomorfizmus $\Rightarrow T^{-1}T = I$ a $TT^{-1} = I$ jsou identity na V_1 a V_2 $\overset{(2),(3)}{\Rightarrow}$ $[T^{-1}].[T] = \boldsymbol{I}_n$ a $[T].[T^{-1}] = \boldsymbol{I}_m$, což podle věty 4.25 znamená, že $[T^{-1}] = [T]^{-1}$.

• Vlastnost (7):

Nechť $\boldsymbol{x} \in V_1$ a $\boldsymbol{y} \in V_2$ jsou libovolné. Protože $[\cdot]$ je unitární, dostáváme užitím 3.90(3):

$\langle T\boldsymbol{x}, \boldsymbol{y}\rangle = \langle [T\boldsymbol{x}], [\boldsymbol{y}]\rangle \overset{(1)}{=} \langle [T].[\boldsymbol{x}], [\boldsymbol{y}]\rangle \overset{4.15(6)}{=} \langle [\boldsymbol{x}], [T]^*.[\boldsymbol{y}]\rangle$,

$\langle \boldsymbol{x}, T^*\boldsymbol{y}\rangle = \langle [\boldsymbol{x}], [T^*\boldsymbol{y}]\rangle \overset{(1)}{=} \langle [\boldsymbol{x}], [T^*].[\boldsymbol{y}]\rangle$.

Pak $\langle T\boldsymbol{x}, \boldsymbol{y}\rangle = \langle \boldsymbol{x}, T^*\boldsymbol{y}\rangle \Rightarrow \langle [\boldsymbol{x}], [T]^*.[\boldsymbol{y}]\rangle = \langle [\boldsymbol{x}], [T^*].[\boldsymbol{y}]\rangle$, kde $[\boldsymbol{x}]$, resp. $[\boldsymbol{y}]$ probíhá všechny prvky $\mathbb{F}^n$, resp. $\mathbb{F}^m$ (totiž $[\cdot]$ je izomorfizmus a tedy surjekce). Adjungovaný operátor je dle 3.82 určen jednoznačně, takže operátory určené maticemi $[T]^*$ a $[T^*]$ jsou stejné. Dle úvodní části důkazu této věty existuje jednojednoznačná korespondence mezi maticemi a příslušnými operátory, takže také $[T]^* = [T^*]$. □

MATHEMATICAL FONTS DEMO (`mathfont.aml`)
(definitions from the input file `mathfont.tex` assumed)

Math roman \mathrm:	$\mathrm{ABCDEFGH}$.
Math roman bold \mathbf:	$\mathbf{ABCDEFGH}$.
Math blackboard bold \mathbb or \Bbb	$\mathbb{ABCDEFGH}$.
Math normal \mathnormal:	$\mathnormal{ABCDEFGH}$.
Math bold normal \bm:	$\boldsymbol{ABCDEFGH}$.
Math italic \mathit:	$\mathit{ABCDEFGH}$.
Math sans serif \mathsf:	$\mathsf{ABCDEFGH}$.
Math typewriter \mathtt:	$\mathtt{ABCDEFGH}$.
Math script \mathcal or \cal:	$\mathcal{ABCDEFGH}$.
Math bold script \bcal:	$\boldsymbol{\mathcal{ABCDEFGH}}$.
Euler script \matheu or \eu:	$\mathscr{ABCDEFGH}$.
Euler bold script \beu:	$\boldsymbol{\mathscr{ABCDEFGH}}$.
Math fraktur \mathfrak or \frak:	$\mathfrak{ABCDEFGH}$.
Math bold fraktur \bfrak:	$\boldsymbol{\mathfrak{ABCDEFGH}}$.
The set of natural numbers \Nset:	$\mathbb{N}$
The set of integers \Zset:	$\mathbb{Z}$
The set of integers modulo N \ZNset{N}:	$\mathbb{Z}_N$
The set of rational numbers \Qset:	$\mathbb{Q}$
The set of real numbers \Rset:	$\mathbb{R}$
The set of complex numbers \Cset:	$\mathbb{C}$

GREEK CHARACTERS (`greek.tex`)

Type:	Print:	Type:	Print:	Type:	Print:
\alpha	α	\beta	β	\gamma	γ
\digamma	$\digamma$	\delta	δ	\epsilon	ϵ
\varepsilon	ε	\zeta	ζ	\eta	η
\theta	θ	\vartheta	ϑ	\iota	ι
\kappa	κ	\varkappa	$\varkappa$	\lambda	λ
\mu	μ	\nu	ν	\xi	ξ
\pi	π	\varpi	ϖ	\rho	ρ
\varrho	ϱ	\sigma	σ	\varsigma	ς
\tau	τ	\upsilon	υ	\phi	ϕ
\varphi	φ	\chi	χ	\psi	ψ
\omega	ω				

Type:	Print:	Type:	Print:
\Gamma	Γ	\varGamma	$\varGamma$
\Delta	Δ	\varDelta	$\varDelta$
\Theta	Θ	\varTheta	$\varTheta$
\Lambda	Λ	\varLambda	$\varLambda$
\Xi	Ξ	\varXi	$\varXi$
\Pi	Π	\varPi	$\varPi$
\Sigma	Σ	\varSigma	$\varSigma$
\Upsilon	Υ	\varUpsilon	$\varUpsilon$
\Phi	Φ	\varPhi	$\varPhi$
\Psi	Ψ	\varPsi	$\varPsi$
\Omega	Ω	\varOmega	$\varOmega$

HEBREW LETTERS (`hebrew.tex`)

Type:	Print:	Type:	Print:
\aleph	$\aleph$	\beth	$\beth$
\daleth	$\daleth$	\gimel	$\gimel$

BINARY OPERATIONS (`binoper.tex`)

Type:	Print:	Type:	Print:
\pm	$\pm$	\mp	$\mp$
\dotplus	$\dotplus$	\cdot	$\cdot$
\times	$\times$	\centerdot	$\centerdot$
\ltimes	$\ltimes$	\rtimes	$\rtimes$
\leftthreetimes	$\leftthreetimes$	\rightthreetimes	$\rightthreetimes$
\ast	$\ast$	\star	$\star$
\diamond	$\diamond$	\circ	$\circ$
\bullet	$\bullet$	\div	$\div$
\setminus	$\setminus$	\smallsetminus	$\smallsetminus$
\cap	$\cap$	\cup	$\cup$
\Cap	$\Cap$	\Cup	$\Cup$
\sqcap	$\sqcap$	\sqcup	$\sqcup$
\wedge	$\wedge$	\vee	$\vee$
\barwedge	$\barwedge$	\doublebarwedge	$\doublebarwedge$
\curlywedge	$\curlywedge$	\curlyvee	$\curlyvee$
\veebar	$\veebar$	\intercal	$\intercal$
\oplus	$\oplus$	\ominus	$\ominus$
\uplus	$\uplus$	\And	$\&$
\otimes	$\otimes$	\oslash	$\oslash$
\odot	$\odot$	\circleddash	$\circleddash$
\circledast	$\circledast$	\circledcirc	$\circledcirc$
\boxminus	$\boxminus$	\boxtimes	$\boxtimes$
\boxdot	$\boxdot$	\boxplus	$\boxplus$
\triangleleft	$\triangleleft$	\triangleright	$\triangleright$
\lhd	$\lhd$	\rhd	$\rhd$
\unlhd	$\unlhd$	\unrhd	$\unrhd$
\bigtriangleup	$\bigtriangleup$	\bigtriangledown	$\bigtriangledown$
\dagger	$\dagger$	\ddagger	$\ddagger$
\wr	$\wr$	\bigcirc	$\bigcirc$
\amalg	$\amalg$	\divideontimes	$\divideontimes$

BIG OPERATORS (`bigoper.tex`)

Type:	Print:	Type:	Print:
\prod_{i=1}^{n}	$\prod_{i=1}^{n}$	\coprod_{i=1}^{n}	$\coprod_{i=1}^{n}$
\bigcap_{i=1}^{n}	$\bigcap_{i=1}^{n}$	\bigcup_{i=1}^{n}	$\bigcup_{i=1}^{n}$
\bigvee_{i=1}^{n}	$\bigvee_{i=1}^{n}$	\bigwedge_{i=1}^{n}	$\bigwedge_{i=1}^{n}$
\bigsqcup_{i=1}^{n}	$\bigsqcup_{i=1}^{n}$	\biguplus_{i=1}^{n}	$\biguplus_{i=1}^{n}$
\bigotimes_{i=1}^{n}	$\bigotimes_{i=1}^{n}$	\bigoplus_{i=1}^{n}	$\bigoplus_{i=1}^{n}$
\bigodot_{i=1}^{n}	$\bigodot_{i=1}^{n}$	\sum_{i=1}^{n}	$\sum_{i=1}^{n}$
\int_a^b	$\int_a^b$	\oint_a^b	$\oint_a^b$
\iint_{E_2}	$\iint_{E_2}$	\iiint_{E_3}	$\iiint_{E_3}$
\iiiint_{E_4}	$\iiiint_{E_4}$	\idotsint_{E_n}	$\idotsint_{E_n}$

$$\prod_{i=1}^{n} \coprod_{i=1}^{n} \bigcap_{i=1}^{n} \bigcup_{i=1}^{n} \bigvee_{i=1}^{n} \bigwedge_{i=1}^{n} \bigsqcup_{i=1}^{n} \biguplus_{i=1}^{n} \bigotimes_{i=1}^{n} \bigoplus_{i=1}^{n} \bigodot_{i=1}^{n} \sum_{i=1}^{n}$$

$$\int_a^b \quad \oint_a^b \quad \iint_{E_2} \quad \iiint_{E_3} \quad \iiiint_{E_4} \quad \idotsint_{E_n}$$

BINARY RELATIONS (`binrel.tex`)

Type:	Print:	Type:	Print:
\leq	$\leq$	\geq	$\geq$
\leqslant	$\leqslant$	\geqslant	$\geqslant$
\eqslantless	$\eqslantless$	\eqslantgtr	$\eqslantgtr$
\lesssim	$\lesssim$	\gtrsim	$\gtrsim$
\lessapprox	$\lessapprox$	\gtrapprox	$\gtrapprox$
\approxeq	$\approxeq$		
\lessdot	$\lessdot$	\gtrdot	$\gtrdot$
\ll	$\ll$	\gg	$\gg$
\lll	$\lll$	\ggg	$\ggg$
\lessgtr	$\lessgtr$	\gtrless	$\gtrless$
\lesseqgtr	$\lesseqgtr$	\gtreqless	$\gtreqless$
\lesseqqgtr	$\lesseqqgtr$	\gtreqqless	$\gtreqqless$
\prec	$\prec$	\succ	$\succ$
\preceq	$\preceq$	\succeq	$\succeq$
\doteqdot	$\doteqdot$	\eqcirc	$\eqcirc$
\circeq	$\circeq$	\fallingdotseq	$\fallingdotseq$
\risingdotseq	$\risingdotseq$	\triangleq	$\triangleq$
\equiv	$\equiv$	\sim	$\sim$
\simeq	$\simeq$	\backsim	$\backsim$
\thicksim	$\thicksim$	\backsimeq	$\backsimeq$
\approx	$\approx$	\thickapprox	$\thickapprox$
\preccurlyeq	$\preccurlyeq$	\succcurlyeq	$\succcurlyeq$
\curlyeqprec	$\curlyeqprec$	\curlyeqsucc	$\curlyeqsucc$
\precsim	$\precsim$	\succsim	$\succsim$
\precapprox	$\precapprox$	\succapprox	$\succapprox$

Type:	Print:	Type:	Print:
\subset	$\subset$	\supset	$\supset$
\subseteq	$\subseteq$	\supseteq	$\supseteq$
\subseteqq	$\subseteqq$	\supseteqq	$\supseteqq$
\Subset	$\Subset$	\Supset	$\Supset$
\sqsubset	$\sqsubset$	\sqsupset	$\sqsupset$
\sqsubseteq	$\sqsubseteq$	\sqsupseteq	$\sqsupseteq$
\vartriangleleft	$\vartriangleleft$	\vartriangleright	$\vartriangleright$
\trianglelefteq	$\trianglelefteq$	\trianglerighteq	$\trianglerighteq$
\vdash	$\vdash$	\dashv	$\dashv$
\vDash	$\vDash$	\Vdash	$\Vdash$
\Vvdash	$\Vvdash$	\models	$\models$
\smile	$\smile$	\smallsmile	$\smallsmile$
\frown	$\frown$	\smallfrown	$\smallfrown$
\mid	$\mid$	\shortmid	$\shortmid$
\parallel	$\parallel$	\shortparallel	$\shortparallel$
\asymp	$\asymp$	\cong	$\cong$
\bumpeq	$\bumpeq$	\Bumpeq	$\Bumpeq$
\between	$\between$	\pitchfork	$\pitchfork$
\propto	$\propto$	\varpropto	$\varpropto$
\bowtie	$\bowtie$	\Join	$\Join$
\in	$\in$	\ni	$\ni$
\backepsilon	$\backepsilon$	\doteq	$\doteq$
\blacktriangleleft	$\blacktriangleleft$	\blacktriangleright	$\blacktriangleright$
\therefore	$\therefore$	\because	$\because$
\perp	$\perp$		

NEGATED BINARY RELATIONS (`nebinrel.tex`)

Type:	Print:	Type:	Print:
\ne	$\ne$	\notin	$\notin$
\nless	$\nless$	\ngtr	$\ngtr$
\nleq	$\nleq$	\ngeq	$\ngeq$
\nleqslant	$\nleqslant$	\ngeqslant	$\ngeqslant$
\nleqq	$\nleqq$	\ngeqq	$\ngeqq$
\lneq	$\lneq$	\gneq	$\gneq$
\lneqq	$\lneqq$	\gneqq	$\gneqq$
\lvertneqq	$\lvertneqq$	\gvertneqq	$\gvertneqq$
\lnsim	$\lnsim$	\gnsim	$\gnsim$
\lnapprox	$\lnapprox$	\gnapprox	$\gnapprox$
\nprec	$\nprec$	\nsucc	$\nsucc$
\npreceq	$\npreceq$	\nsucceq	$\nsucceq$
\precneqq	$\precneqq$	\succneqq	$\succneqq$
\precnsim	$\precnsim$	\succnsim	$\succnsim$
\precnapprox	$\precnapprox$	\succnapprox	$\succnapprox$
\nsim	$\nsim$	\ncong	$\ncong$
\nshortmid	$\nshortmid$	\nshortparallel	$\nshortparallel$
\nmid	$\nmid$	\nparallel	$\nparallel$
\nvdash	$\nvdash$	\nvDash	$\nvDash$
\nVdash	$\nVdash$	\nVDash	$\nVDash$
\ntriangleleft	$\ntriangleleft$	\ntriangleright	$\ntriangleright$
\ntrianglelefteq	$\ntrianglelefteq$	\ntrianglerighteq	$\ntrianglerighteq$

Type:	Print:	Type:	Print:
\nsubseteq	$\nsubseteq$	\nsupseteq	$\nsupseteq$
\nsubseteqq	$\nsubseteqq$	\nsupseteqq	$\nsupseteqq$
\subsetneq	$\subsetneq$	\supsetneq	$\supsetneq$
\varsubsetneq	$\varsubsetneq$	\varsupsetneq	$\varsupsetneq$
\subsetneqq	$\subsetneqq$	\supsetneqq	$\supsetneqq$
\varsubsetneqq	$\varsubsetneqq$	\varsupsetneqq	$\varsupsetneqq$

To put a slash through a symbol type **not** before it, e.g. \not= gives $\neq$.

ARROWS (`arrows.tex`)

Type:	Print:	Type:	Print:
\leftarrow	$\leftarrow$	\rightarrow or \to	$\rightarrow$
\longleftarrow	$\longleftarrow$	\longrightarrow	$\longrightarrow$
\Leftarrow	$\Leftarrow$	\Rightarrow	$\Rightarrow$
\Longleftarrow	$\Longleftarrow$	\Longrightarrow	$\Longrightarrow$
\leftrightarrow	$\leftrightarrow$	\longleftrightarrow	$\longleftrightarrow$
\Leftrightarrow	$\Leftrightarrow$	\Longleftrightarrow	$\Longleftrightarrow$
\leftleftarrows	$\leftleftarrows$	\rightrightarrows	$\rightrightarrows$
\leftrightarrows	$\leftrightarrows$	\rightleftarrows	$\rightleftarrows$
\Lleftarrow	$\Lleftarrow$	\Rrightarrow	$\Rrightarrow$
\twoheadleftarrow	$\twoheadleftarrow$	\twoheadrightarrow	$\twoheadrightarrow$
\leftarrowtail	$\leftarrowtail$	\rightarrowtail	$\rightarrowtail$
\looparrowleft	$\looparrowleft$	\looparrowright	$\looparrowright$
\uparrow	$\uparrow$	\downarrow	$\downarrow$
\Uparrow	$\Uparrow$	\Downarrow	$\Downarrow$
\upuparrows	$\upuparrows$	\downdownarrows	$\downdownarrows$
\updownarrow	$\updownarrow$	\Updownarrow	$\Updownarrow$
\nearrow	$\nearrow$	\searrow	$\searrow$
\swarrow	$\swarrow$	\nwarrow	$\nwarrow$
\mapsto	$\mapsto$	\longmapsto	$\longmapsto$
\hookleftarrow	$\hookleftarrow$	\hookrightarrow	$\hookrightarrow$
\leftharpoonup	$\leftharpoonup$	\rightharpoonup	$\rightharpoonup$
\leftharpoondown	$\leftharpoondown$	\rightharpoondown	$\rightharpoondown$
\upharpoonleft	$\upharpoonleft$	\upharpoonright	$\upharpoonright$
\downharpoonleft	$\downharpoonleft$	\downharpoonright	$\downharpoonright$
\multimap	$\multimap$	\rightsquigarrow	$\rightsquigarrow$
\leftrightsquigarrow	$\leftrightsquigarrow$	\leadsto	$\leadsto$

Type:	Print:	Type:	Print:
\nleftarrow	$\nleftarrow$	\nrightarrow	$\nrightarrow$
\nLeftarrow	$\nLeftarrow$	\nRightarrow	$\nRightarrow$
\nleftrightarrow	$\nleftrightarrow$	\nLeftrightarrow	$\nLeftrightarrow$

MISCELLANEOUS SYMBOLS (`miscell.tex`)

Type:	Print:	Type:	Print:
\hbar	$\hbar$	\hslash	$\hslash$
\imath	$\imath$	\jmath	$\jmath$
\ell	ℓ	\complement	$\complement$
\wp	$\wp$	\Re	Re
\Im	Im	\partial	∂
\infty	∞	\smallint	$\smallint$
\P	¶	\S	§
\prime	$\prime$	\backprime	$\backprime$
\emptyset	$\emptyset$	\varnothing	$\varnothing$
\Bbbk	$\Bbbk$	\backslash	$\backslash$
\diagup	$\diagup$	\diagdown	$\diagdown$
\triangle	$\triangle$	\nabla	∇
\vartriangle	$\vartriangle$	\blacktriangle	$\blacktriangle$
\triangledown	$\triangledown$	\blacktriangledown	$\blacktriangledown$
\square	$\square$	\lozenge	$\lozenge$
\Box	$\Box$	\Diamond	$\Diamond$
\blacksquare	$\blacksquare$	\blacklozenge	$\blacklozenge$
\forall	$\forall$	\exists	$\exists$
\nexists	$\nexists$	\neg	$\neg$
\angle	$\angle$	\sphericalangle	$\sphericalangle$
\measuredangle	$\measuredangle$	\\|	$\\|$
\surd	$\surd$	\Vert	$\Vert$
\top	$\top$	\bot	$\bot$
\dag	†	\ddag	‡
\flat	$\flat$	\natural	$\natural$
\sharp	$\sharp$		
\clubsuit	$\clubsuit$	\diamondsuit	$\diamondsuit$
\heartsuit	$\heartsuit$	\spadesuit	$\spadesuit$
\circledS	$\circledS$	\bigstar	$\bigstar$
\mho	$\mho$	\eth	$\eth$
\Finv	$\Finv$	\Game	$\Game$

Additional symbols can be made by stacking one symbol on top of another with the **stackrel** command, e.g. $A \stackrel{\alpha}{\rightarrow} B$ gives $A \stackrel{\alpha}{\rightarrow} B$.

D.1. Důkaz věty 2.19:
Nechť $a, b \in M$ jsou libovolné prvky.
$\boxed{\text{I.}}$ Ukážeme, že $<$ je areflexivní a symetrická, je-li $\leq$ uspořádání (reflexivní, antisymetrická a tranzitivní relace):
areflexivita: $(a \leq a) \wedge (a \neq a)$ neplatí $\Rightarrow a \not< a$
tranzitivita: $(a < b) \wedge (b < c) \Rightarrow (a \leq b) \wedge (b \leq c) \wedge (a \neq b) \wedge (b \neq c) \Rightarrow a \leq c$ v důsledku tranzitivity relace $\leq$ a $a \neq c$ v důsledku její antisymetrie (kdyby $a = c$, pak $a = b$ je v rozporu s $a \neq b$); tedy platí $(a \leq c) \wedge (a \neq c)$ neboli $a < c$.
$\boxed{\text{II.}}$ Ukážeme, že $\leq$ je reflexivní, antisymetrická a tranzitivní, je-li $<$ areflexivní a tranzitivní relace:
reflexivita: $(a < a) \vee (a = a)$ platí $\Rightarrow a \leq a$
tranzitivita: $(a \leq b) \wedge (b \leq c) \Rightarrow ((a < b) \vee (a = b)) \wedge ((a < b) \wedge (b = c))$ a odtud pro všechny čtyři možné případy:
a) $a = b, b = c \Rightarrow a = c \Rightarrow a \leq c$
b) $a = b, b < c \Rightarrow a < c \Rightarrow a \leq c$
c) $a < b, b = c \Rightarrow a < c \Rightarrow a \leq c$
d) $a < b, b < c \Rightarrow a < c$ (tranzitivita $<$) $\Rightarrow a \leq c$.
antisymetrie: $(a \leq b) \wedge (b \leq a) \Rightarrow a \leq a$ v důsledku již dokázané tranzitivity $\Rightarrow (a < a) \vee (a = a)$, přičemž $a < a$ nemůže nastat (areflexivita $<$), a tedy platí $a = a$. $\square$

D.2. DŮKAZ věty 2.21:
(1) jsou-li a, a' dva takové prvky, pak platí současně $a \leq a'$ i $a' \leq a$ a tedy $a = a'$ v důsledku antisymetrie.
(2) a nejmenší $\Rightarrow x \geq a \; \forall x \in M \Rightarrow$ v M neexistuje $x < a$ a tedy a je minimální v M.
(3) sporem: kdyby existovaly dva takové prvky $a \neq a'$, pak vzhledem k úplnému uspořádání množiny M platí $a < a'$ nebo $a' < a$, takže alespoň jeden z prvků a, a' nemůže být maximální, resp. minimální.
(4) sporem: kdyby například neexistoval minimální prvek, pak v M lze vybrat nekonečnou posloupnost prvků $a_1 > a_2 > a_3 > \dots$ (a_1

vybereme libovolně, protože není minimální, existuje $a_2 < a_1$, ten také není minimální, atd.), což je spor s konečností množiny M. $\square$

D.3. Důkaz věty 2.23:
$\boxed{\Leftarrow}$ tato implikace plyne z tranzitivity relace $<$
$\boxed{\Rightarrow}$ je-li $a < b$ v konečné množině M, pak její uspořádaná podmnožina $A_0 := \{c \in M \,|\, a < c \leq b\}$ je rovněž konečná a dle věty 2.21(4) má alespoň jeden minimální prvek t_1. Pokud $t_1 < b$ vezmeme minimální prvek t_2 podmnožiny $A_1 := \{c \in M \,|\, t_1 < c \leq b\}$, atd. Vzhledem ke konečnosti množiny M musí po konečném počtu n kroků nastat případ $t_n = b$. $\square$

D.4. DŮKAZ nerovnosti z definice 2.26:
Důkaz probíhá ve třech návazných krocích:
$\boxed{\text{I.}}$ Nejprve ukážeme, že $b_k^- \leq b_N^+$ pro každé $k, N \in \mathbb{N}$:
$\boxed{\text{II.}}$ Ukážeme, že $\limsup a_n$ je horní závora posloupnosti $\{b_k^-\}_{k\in\mathbb{N}}$:
$\boxed{\text{III.}}$ Ověříme požadovanou nerovnost $\liminf a_n \leq \limsup a_n$:
$\square$

D.5. DŮKAZ věty 2.27:
(1) pro neklesající posloupnost $\{a_n\}$ je $b_k^+ = \sup\{a_n\}_{n=k}^\infty = \sup\{a_n\}_{n=1}^\infty$ konstantní posloupnost, jejíž infimum (=$\limsup\{a_n\}_{n=1}^\infty$) je tatáž konstanta $\sup\{a_n\}_{n=1}^\infty$. Podobně $b_k^- = \inf\{a_n\}_{n=k}^\infty = a_k$, takže opět $\liminf\{a_n\}_{n=1}^\infty = \sup\{b_k^-\}_{k=1}^\infty = \sup\{a_k\}_{k=1}^\infty$.
(2) se dokazuje analogicky. $\square$

D.6. Důkaz věty 2.29:
Tvrzení dokážeme pro supremum (postup pro infimum je analogický).
$\boxed{\Rightarrow}$ $a = \sup P$ existuje $\Rightarrow a \geq x \forall x \in P \Rightarrow f(a) \geq f(x) \forall f(x) \in f(P)$ $\Rightarrow f(a)$ je horní závora $f(P)$. Je-li naopak $t \in N$ nějaká horní závora $f(P)$, pak $t \geq f(x) \forall x \in P \Rightarrow f^{-1}(t) \geq f^{-1}f(x) = x \forall x \in P \Rightarrow$ $f^{-1}(t)$ je horní závora $P \Rightarrow f^{-1}(t) \geq a \Rightarrow t = ff^{-1}(t) \geq f(a) \Rightarrow$ $f(a) = \sup f(P)$ existuje.
$\boxed{\Leftarrow}$ Implikace [$\sup f(P)$ existuje $\Rightarrow \sup P$ existuje] plyne z předchozího záměnou $f \leftrightarrow f^{-1}$ a $P \leftrightarrow f(P)$. $\square$

D.7. DŮKAZ věty 2.34:
Pro zavedenou relaci ρ ověříme, že má vlastnosti ekvivalence:
reflexivita: $a \in M = \bigcup_{i \in I} M_i \Rightarrow \exists\, i \in I : a \in M_i \Rightarrow a\rho a$.
tranzitivita: $a\rho b$, $b\rho c \Rightarrow \exists\, i, j \in I : a, b \in M_i; b, c \in M_j \Rightarrow b \in M_i \cap M_j$ $\Rightarrow i = j$, neboť $M_i \cap M_j = \emptyset$ pro $i \neq j \Rightarrow a, c \in M_i \Rightarrow a\rho c$.
symetrie: $a\rho b \Rightarrow \exists\, i \in I : a, b \in M_i \Rightarrow \exists\, i \in I : b, a \in M_i \Rightarrow b\rho a$. □

D.8. DŮKAZ věty 2.35:
Pro každé $a \in M$ položme $M_a := \{x \in M \mid x\rho a\}$ (podmnožina všech prvků v M ekvivalentních s x) a $\overline{M} := \{M_a\}_{a \in M}$. Ukážeme, že $\overline{M}$ je rozklad na množině M:
• $M \neq \emptyset \Rightarrow \exists\, a \in M \Rightarrow a \in M_a \in \overline{M} \Rightarrow \overline{M} \neq \emptyset$ a $M_a \neq \emptyset$ pro každé $M_a \in \overline{M}$.
• pro každé $a \in M$ je $a \in M_a$ a $M_a \subseteq M$, takže platí $M \subseteq \bigcup_{a \in M} \subseteq M$ a tedy $M = \bigcup_{a \in M}$.
• $M_a \cap M_b \neq \emptyset \Rightarrow \exists\, c \in M_a \cap M_b \Rightarrow a\rho c, c\rho b$. Pak $x \in M_a \Rightarrow x\rho a \Rightarrow x\rho b$ v důsledku tranzitivity, neboť je $x\rho a\rho c\rho b \Rightarrow x \in M_b$ a tedy jsme dokázali $M_a \subseteq M_b$. Záměnou role a a b analogicky platí též $M_b \subseteq M_a$. Celkem tedy $M_a = M_b$. Závěr: dvě množiny z $\overline{M}$ jsou buď disjunktní a nebo stejné.
• Celkem jsme tedy ukázali, že $\overline{M}$ tvoří na M rozklad (po vynechání duplicitních množin). Zřejmě platí $x\rho y \iff x, y \in M_x$. □

D.9. Důkaz věty 2.38:
f je prosté: $\Theta_1, \Theta_2 \in E(M), \Theta_1 \neq \Theta_2 \Rightarrow \exists\, [x, y] \in \Theta_1 - \Theta_2$ nebo $[x, y] \in \Theta_2 - \Theta_1$. Nechť například $[x, y] \in \Theta_1 - \Theta_2$. Pak
$x, y \in M_x^1 \in M/\Theta_1$, $x \in M_x^2 \in M/\Theta_2$, ale $y \notin M_x^2 \Rightarrow M_x^1 \neq M_x^2 \Rightarrow$
v příslušných rozkladech existují alespoň dvě různé třídy, takže rozklady jsou různé množiny: $f(\theta_1) = M/\Theta_1 \neq M/\Theta_2 = f(\Theta_2)$.
f je surjekce: je přímým důsledke věty 2.34
Zatím jsme tedy ukázali, že f je bijekce.
f je monotonní: $\Theta_1 \subseteq \Theta_2 \Rightarrow M_x^1 := \{y \mid y\Theta_1 x\} \subseteq M_x^2 := \{z \mid z\Theta_2 x\}$ pro každé $x \in M$ (tj. pro všechny třídy z M/Θ_1) $\Rightarrow f(\Theta_1) \leq f(\Theta_2)$.
f^{-1} je monotonní: nechť naopak $f(\Theta_1) \leq f(\Theta_2)$ a $x\Theta_1 y$ pro nějaká

$x, y \in M$. Pak $y \in M_x^1 \subseteq M_x^2 \Rightarrow x\Theta_2 y$ a tedy $\Theta_1 \subseteq \Theta_2$.
Celkem f je izomorfizmus uspořádaných množin. $\square$

D.10. <u>DŮKAZ věty 2.39</u>:

<u>reflexivita</u>: $f(x) = f(x) \Rightarrow x \overset{f}{\sim} x$

<u>symetrie</u>: $x \overset{f}{\sim} y \Rightarrow f(x) = f(y) \Rightarrow f(y) = f(x) \Rightarrow y \overset{f}{\sim} x$

<u>tranzitivita</u>: $x \overset{f}{\sim} y$, $y \overset{f}{\sim} z \Rightarrow f(x) = f(y)$, $f(y) = f(z) \Rightarrow f(x) = f(z)$
$\Rightarrow x \overset{f}{\sim} z$. $\square$

D.11. <u>DŮKAZ důsledku 2.41</u>:

$x \overset{f}{\sim} y \Rightarrow f(x) = f(y) \Rightarrow g(f(x)) = g(f(y)) \Rightarrow (gf)(x) = (gf)(y) \Rightarrow$
$x \overset{gf}{\sim} y$. $\square$

D.12. Důkaz věty 2.43:

$\boxed{\text{I.}}$ Nechť $\sim$ je kongruence na M:
• Je-li $\rho \in \mathcal{S}$ nějaká n-ární relace, pak
$\rho(a_1, \ldots, a_n) = 1 \Rightarrow \overline{\rho}(\overline{a}_1, \ldots, \overline{a}_n) = 1$ dle 2.42(i) a tedy zobrazení „pruh nahoře“ je podle 2.10(1) homomorfizmem vzhledem k ρ.
• Je-li $\omega \in \mathcal{S}$ nějaká n-ární operace, pak $\overline{\omega}(\overline{a}_1, \ldots, \overline{a}_n) = \overline{\omega(a_1, \ldots, a_n)}$ dle 2.42(ii) a tedy zobrazení „pruh nahoře“ je podle 2.10(2) homomorfizmem vzhledem k ω.

$\boxed{\text{II.}}$ Naopak nechť f je homomorfizmus, pak $a_1 \overset{f}{\sim} b_1, \ldots, a_n \overset{f}{\sim} b_n \Rightarrow$ $f(a_i) = f(b_i)$ pro $i = 1, \ldots, n \Rightarrow f(\omega(a_1, \ldots, a_n)) = \omega(f(a_1), \ldots, f(a_n))$ $= \omega(f(b_1), \ldots, f(b_n)) = f(\omega(b_1, \ldots, b_n))$ pro libovolnou n-ární operaci $\omega \Rightarrow \omega(a_1, \ldots, a_n) \overset{f}{\sim} \omega(b_1, \ldots, b_n) \Rightarrow \overset{f}{\sim}$ je kongruence. $\square$

D.13. DŮKAZ věty 3.3:

(L5) $\boxed{\Leftarrow}$

a) $\underline{\alpha = 0}$: $\boldsymbol{x} \overset{L4}{=} 1\boldsymbol{x} = (1+0)\boldsymbol{x} \overset{L2}{=} 1\boldsymbol{x} + 0\boldsymbol{x} \overset{L4}{=} \boldsymbol{x} + 0\boldsymbol{x} \Rightarrow$
$\mathbf{0} = -\boldsymbol{x} + \boldsymbol{x} = -\boldsymbol{x} + (\boldsymbol{x} + 0\boldsymbol{x}) = (-\boldsymbol{x} + \boldsymbol{x}) + 0\boldsymbol{x} = \mathbf{0} + 0\boldsymbol{x} = 0\boldsymbol{x}$.

b) $\underline{\boldsymbol{x} = \mathbf{0}}$: $\boldsymbol{y} = \boldsymbol{y} + \mathbf{0} \Rightarrow \alpha\boldsymbol{y} = \alpha(\boldsymbol{y} + \mathbf{0}) \overset{L1}{=} \alpha\boldsymbol{y} + \alpha\mathbf{0} \Rightarrow$
$\mathbf{0} = -\alpha\boldsymbol{y} + \alpha\boldsymbol{y} = -\alpha\boldsymbol{y} + (\alpha\boldsymbol{y} + \alpha\mathbf{0}) = (-\alpha\boldsymbol{y} + \alpha\boldsymbol{y}) + \alpha\mathbf{0} = \mathbf{0} + \alpha\mathbf{0} = \alpha\mathbf{0}$.

(L5) $\boxed{\Rightarrow}$ Jestliže $\alpha\boldsymbol{x} = \mathbf{0}$, pak nastanou 2 případy:
a) $\underline{\alpha = 0}$, kdy tvrzení platí, nebo
b) $\underline{\alpha \neq 0}$, kdy $\boldsymbol{x} \overset{L4}{=} 1\boldsymbol{x} = (\alpha^{-1}\alpha)\boldsymbol{x} \overset{L3}{=} \alpha^{-1}(\alpha\boldsymbol{x}) = \alpha^{-1}\mathbf{0} = \mathbf{0}$ dle předchozí části důkazu.

(L6)
$(-\alpha)\boldsymbol{x} + \alpha\boldsymbol{x} \overset{L2}{=} (-\alpha + \alpha)\boldsymbol{x} = 0\boldsymbol{x} \overset{L5}{=} \mathbf{0}$,
$\alpha(-\boldsymbol{x}) + \alpha\boldsymbol{x} \overset{L1}{=} \alpha(-\boldsymbol{x} + \boldsymbol{x}) = \alpha\mathbf{0} \overset{L5}{=} \mathbf{0}$,
Prvek opačný k $\alpha\boldsymbol{x}$ je jediný, takže $-\alpha\boldsymbol{x} = \alpha(-\boldsymbol{x}) = (-\alpha)\boldsymbol{x}$.

(L7) $\alpha(\boldsymbol{x}-\boldsymbol{y}) = \alpha(\boldsymbol{x}+(-\boldsymbol{y})) \overset{L1}{=} \alpha\boldsymbol{x}+\alpha(-\boldsymbol{y}) \overset{L6}{=} \alpha\boldsymbol{x}+(-\alpha\boldsymbol{y}) = \alpha\boldsymbol{x}-\alpha\boldsymbol{y}$.

(L8) $(\alpha-\beta)\boldsymbol{x} = (\alpha+(-\beta))\boldsymbol{x} \overset{L2}{=} \alpha\boldsymbol{x}+(-\beta)\boldsymbol{x} \overset{L6}{=} \alpha\boldsymbol{x}+(-\beta\boldsymbol{x}) = \alpha\boldsymbol{x}-\beta\boldsymbol{x}$.

(L9) Opakovaně aplikujeme axiom L1 s využitím asociativity sečítání v grupě $(V, +, \mathbf{0})$.

(L10) Opakovaně aplikujeme axiom L2 s využitím asociativity sečítání v aditivní grupě ($\mathbb{F}$,+ ,0).

(L11)
$\left(\sum_{i=1}^m \alpha_i\right)\left(\sum_{j=1}^n \boldsymbol{x}_j\right) \overset{L10}{=} \sum_{i=1}^m \alpha_i \sum_{j=1}^n \boldsymbol{x}_j = \alpha_1(\boldsymbol{x}_1 + \cdots + \boldsymbol{x}_n) + \cdots$
$+\alpha_m(\boldsymbol{x}_1+\cdots+\boldsymbol{x}_n) \overset{L9}{=} \alpha_1\boldsymbol{x}_1+\cdots+\alpha_1\boldsymbol{x}_n+\cdots+\alpha_m\boldsymbol{x}_1+\cdots+\alpha_m\boldsymbol{x}_n =$
$\sum_{i=1}^m \sum_{j=1}^n \alpha_i\boldsymbol{x}_j$, kde poslední rovnost je důsledkem komutativity sečítání v grupě $(V, +, \mathbf{0})$. Poslední dokazovanou rovnost dostaneme analogicky užitím L10 místo L9 (místo α_i před součet vektorů v závorce vytýkáme $\boldsymbol{x}_j$ za součet skalárů v závorce). □

D.14. DŮKAZ věty 3.7:

$\boxed{\Rightarrow}$ sečítání a násobení skaláry jsou operacemi struktury $\mathcal{L}_{\mathbb{F}}$ a tudíž podprostor k nim musí být uzavřen.

$\boxed{\Leftarrow}$ Platí-li (1) a (2), je třeba ještě ověřit uzavřenost ke zbývajícím grupovým operacím v grupě $(V, +, \mathbf{0})$ (tj. vlastnosti (2) a (3) z poznámky 2.58(2)(3)):
• Jelikož $W \neq \emptyset$, tak existuje $\boldsymbol{x} \in W$ a užitím (2) a L5 dostáváme $\mathbf{0} = 0\boldsymbol{x} \in W$.
• Pro $\boldsymbol{x} \in W$ analogicky užitím (2) a L6 dostáváme $-\boldsymbol{x} = (-1)\boldsymbol{x} \in W$. $\square$

D.15. DŮKAZ důsledku 3.8:
$\alpha_i \boldsymbol{x}_i \in W \ \forall i \in I$ dle (1) a jejich součet tedy rovněž leží ve W podle obecného asociativního zákona 2.46. $\square$

D.16. DŮKAZ věty 3.10:
Pro $\bigcap_{i \in I} W_i$ je třeba ověřit vlastnosti (1) a (2) z věty 3.7:

(1) $\boldsymbol{x}, \boldsymbol{y} \in \bigcap_{i \in I} W_i \Rightarrow \boldsymbol{x}, \boldsymbol{y} \in W_i \ \forall i \in I \overset{(1)}{\Rightarrow} \boldsymbol{x} + \boldsymbol{y} \in W_i \ \forall i \in I \Rightarrow \boldsymbol{x} + \boldsymbol{y} \in \bigcap_{i \in I} W_i$.

(2) $\boldsymbol{x} \in \bigcap_{i \in I} W_i \Rightarrow \boldsymbol{x} \in W_i \ \forall i \in I \overset{(2)}{\Rightarrow} \alpha \boldsymbol{x} \in W_i \ \forall i \in I$ a $\alpha \in \mathbb{F} \Rightarrow \alpha \boldsymbol{x} \in \bigcap_{i \in I} W_i$. $\square$

D.17. DŮKAZ věty 3.12:
(1) Položme $W(G) := \bigcap \{W \mid W$ je podprostor ve $V : G \subseteq W\}$. Potom $W(G)$ je podprostor ve V dle 3.10. Z jeho konstrukce plyne $G \subseteq W(G) \subseteq W$ pro každý podprostor W obsahující G. $W(G)$ je tedy nejmenší a tudíž $\mathcal{L}(G) = W(G)$.
Je-li $G = \emptyset$, pak nutně $W(G) = \{\mathbf{0}\}$, neboť $\mathbf{0}$ je prvkem každého podprostoru a $\{\mathbf{0}\}$ je nejmenší z nich dle poznámky 3.9, přičemž $\emptyset \subseteq \{\mathbf{0}\}$ platí triviálně.
(2) Položme $L(G) := \{\sum_{i=1}^{n} \alpha_i \boldsymbol{x}_i \mid \alpha_i \in \mathbb{F}, \boldsymbol{x}_i \in G, n \in \mathbb{N}\}$. Pak platí:
• $G \subseteq L(G)$, neboť pro každé $\boldsymbol{x} \in G$ je $\boldsymbol{x} = 1\boldsymbol{x} \in L(G)$.
• $L(G)$ je podprostor dle 3.7, neboť součet dvou lineárních kombinací prvků z G je opět lineární kombinace prvků z G. Podobně pro skalární násobek: $\alpha(\alpha_1 \boldsymbol{x}_1 + \cdots + \alpha_n \boldsymbol{x}_n) \overset{L9}{=} \alpha(\alpha_1 \boldsymbol{x}_1) + \cdots + \alpha(\alpha_n \boldsymbol{x}_n) \overset{L3}{=} (\alpha\alpha_1)\boldsymbol{x}_1 + \cdots + (\alpha\alpha_n)\boldsymbol{x}_n$.
Tedy $L(G)$ je podprostor obsahující G a protože $\mathcal{L}(G)$ je nejmenší

takový, tak musí platit $\mathcal{L}(G) \subseteq L(G)$.
Podle 3.8 musí být $\mathcal{L}(G)$ uzavřen ke všem lineárním kombinacím svých prvků, tedy zejména i těch z G, takže také platí opačná inkluze $L(G) \subseteq \mathcal{L}(G)$. Celkem jsme tak ukázali $\mathcal{L}(G) = L(G)$. $\square$

D.18. DŮKAZ věty 3.14:
(1) $\mathcal{L}(G)$ je podprostor $\stackrel{3.9}{\Rightarrow} \{\mathbf{0}\} \subseteq \mathcal{L}(G) \Rightarrow \mathbf{0} \in \mathcal{L}(G)$.
(2) Mohou nastat 2 případy:
• $M = \emptyset$, kdy $\{\mathbf{0}\} = \mathcal{L}(M) \subseteq \mathcal{L}(G)$ dle (1).
• $M \neq \emptyset$, $M \subseteq \mathcal{L}(G)$, kdy dle 3.8 každá lineární kombinace prvků z M padne do $\mathcal{L}(G)$, takže s uvážením 3.12(2) dostáváme $\mathcal{L}(M) \subseteq \mathcal{L}(G)$.
(3) Postupujeme analogicky jako v předchozím případě:
• $M = \emptyset \Rightarrow \{\mathbf{0}\} = \mathcal{L}(M) \subseteq \mathcal{L}(N)$ dle (1).
• $M \neq \emptyset$, $M \subseteq N \Rightarrow$ dle 3.8 každá lineární kombinace prvků z M je současně také lineární kombinací prvků z N, takže opět s uvážením 3.12(2) dostáváme $\mathcal{L}(M) \subseteq \mathcal{L}(N)$.
(4) Inkluze $W \subseteq \mathcal{L}(W)$ je přímo z definice 3.11. Naopak nechť $\boldsymbol{x} \in \mathcal{L}(W)$ je libovolný prvek. Protože $W \neq \emptyset$, je dle 3.12(2) $\boldsymbol{x} = \sum_{i=1}^{n} \alpha_i \boldsymbol{x}_i$, kde $\boldsymbol{x}_i \in W$, takže $\boldsymbol{x} \in W$ dle 3.8. Tedy také platí opačná inkluze $\mathcal{L}(G) \subseteq W$ a celkem $\mathcal{L}(G) = W$.
(5) $G - \{\boldsymbol{x}\} \subset G \stackrel{(3)}{\Rightarrow} \mathcal{L}(G - \{\boldsymbol{x}\}) \subseteq \mathcal{L}(G)$.
Naopak: $\boldsymbol{x} \in \mathcal{L}(G - \{\boldsymbol{x}\}) \Rightarrow G = (G - \{\boldsymbol{x}\}) \cup \{\boldsymbol{x}\} \subseteq \mathcal{L}(G - \{\boldsymbol{x}\}) \stackrel{(2)}{\Rightarrow} \mathcal{L}(G) \subseteq \mathcal{L}(G - \{\boldsymbol{x}\})$.
Celkem jsme dokázali $\mathcal{L}(G) = \mathcal{L}(G - \{\boldsymbol{x}\})$.
(6) $(G - \{\boldsymbol{x}\}) \cup \{\alpha \boldsymbol{x}\} \subseteq \mathcal{L}(G) \stackrel{(2)}{\Rightarrow} \mathcal{L}((G - \{\boldsymbol{x}\}) \cup \{\alpha \boldsymbol{x}\}) \subseteq \mathcal{L}(G)$.
Naopak: $G = (G - \{\boldsymbol{x}\}) \cup \{\alpha^{-1}(\alpha \boldsymbol{x})\} \subseteq \mathcal{L}((G - \{\boldsymbol{x}\}) \cup \{\alpha \boldsymbol{x}\}) \stackrel{(2)}{\Rightarrow} \mathcal{L}(G) \subseteq \mathcal{L}((G - \{\boldsymbol{x}\}) \cup \{\alpha \boldsymbol{x}\})$.
Celkem jsme dokázali $\mathcal{L}(G) = \mathcal{L}((G - \{\boldsymbol{x}\}) \cup \{\alpha \boldsymbol{x}\})$.
(7) $(G - \{\boldsymbol{x}\}) \cup \{\boldsymbol{x} + \boldsymbol{y}\} \subseteq \mathcal{L}(G) \stackrel{(2)}{\Rightarrow} \mathcal{L}((G - \{\boldsymbol{x}\}) \cup \{\boldsymbol{x} + \boldsymbol{y}\}) \subseteq \mathcal{L}(G)$.
Naopak: $G = (G - \{\boldsymbol{x}\}) \cup \{\boldsymbol{x} + \boldsymbol{y} - \boldsymbol{y}\} \subseteq \mathcal{L}((G - \{\boldsymbol{x}\}) \cup \{\boldsymbol{x} + \boldsymbol{y}\}) \stackrel{(2)}{\Rightarrow} \mathcal{L}(G) \subseteq \mathcal{L}((G - \{\boldsymbol{x}\}) \cup \{\boldsymbol{x} + \boldsymbol{y}\})$.
Celkem jsme dokázali $\mathcal{L}(G) = \mathcal{L}((G - \{\boldsymbol{x}\}) \cup \{\boldsymbol{x} + \boldsymbol{y}\})$. $\square$

D.19. DŮKAZ věty 3.17:
(1) Nechť $\emptyset \neq N \subseteq M$. Vyšetříme dva případy:
a) $\underline{M \text{ nekonečná lineárně nezávislá}}$: Všechny konečné podmnožiny v N jsou také konečnými podmnožinami v M a jsou proto lineárně nezávislé, když M je lineárně nezávislá.
b) $\underline{M =: \{x_1, \dots, x_n\} \text{ konečná lineárně nezávislá}}$: bez újmy na obecnosti můžeme položit $N := \{x_1, \dots, x_k\}, k \leq n$. Pak $\mathbf{0} = \alpha_1 \boldsymbol{x}_1 + \dots + \alpha_k \boldsymbol{x}_k + 0\boldsymbol{x}_{k+1} + \dots + 0\boldsymbol{x}_n \Rightarrow \alpha_1 = \dots = \alpha_k = 0$, neboť M je lineárně nezávislá. Tedy rovněž N je lineárně nezávislá.

(2) $1 \cdot \mathbf{0} = \mathbf{0}$, kde $1 \neq 0 \Rightarrow \{\mathbf{0}\}$ není lineárně nezávislá $\overset{(1)}{\Rightarrow} \{\mathbf{0}\} \nsubseteq M$ $\Rightarrow \mathbf{0} \notin M$.

(3) $\mathbf{0} = \boldsymbol{x} - \boldsymbol{x} = \sum_{i=1}^n \alpha_i \boldsymbol{x}_i - \sum_{i=1}^n \beta_i \boldsymbol{x}_i \overset{(*)}{=} \sum_{i=1}^n (\alpha_i \boldsymbol{x}_i - \beta_i \boldsymbol{x}_i) \overset{L7}{=} \sum_{i=1}^n (\alpha_i - \beta_i)\boldsymbol{x}_i \Rightarrow \alpha_i - \beta_i = 0$ pro $i = 1, \dots, n \Rightarrow \alpha_i = \alpha_i - \beta_i + \beta_i = 0 + \beta_i = \beta_i$ pro $i = 1, \dots, n$. Na závěr poznamenejme, že rovnost $(*)$ platí vzhledem ke komutativitě a asociativitě sečítání.

(4) Tvrzení je důsledkem (1) a (3). Sporem: kdyby totiž existovala dvě různá vyjádření $\boldsymbol{x} = \sum_{i=1}^n \alpha_i \boldsymbol{x}_i = \sum_{j=1}^m \beta_j \boldsymbol{y}_j$, kde $\boldsymbol{x}_i, \boldsymbol{y}_j \in M$ a $\alpha_i \neq 0, \beta_j \neq 0$ $(i = 1, \dots, n,\ j = 1, \dots, m)$, pak vhodným doplněním nulových koeficientů tato vyjádření lze přepsat jako dvě navzájem různé lineární kombinace vektorů z konečné podmnožiny $N := \{\boldsymbol{x}_1, \dots, \boldsymbol{x}_n\} \cup \{\boldsymbol{y}_1, \dots, \boldsymbol{y}_m\}$. Podle (3) toto není možné (spor), neboť N je dle (1) lineárně nezávislá. □

D.20. DŮKAZ věty 3.18:
$\emptyset \neq M \subseteq V$ je lineárně závislá $\Leftrightarrow$ M není lineárně nezávislá $\Leftrightarrow$ v M existuje neprázdná konečná podmnožina $N = \{\boldsymbol{x}_1, \dots, \boldsymbol{x}_n\}$, která rovněž není lineárně nezávislá (srov. 3.16 a 3.17(1)) $\Leftrightarrow$ $\mathbf{0} = \alpha_1 \boldsymbol{x}_1 + \dots + \alpha_n \boldsymbol{x}_n$, kde $\alpha_i \neq 0$ pro nějaké i $\Leftrightarrow$ $\alpha_i \boldsymbol{x}_i = -\alpha_1 \boldsymbol{x}_1 - \dots - \alpha_{i-1}\boldsymbol{x}_{i-1} - \alpha_{i+1}\boldsymbol{x}_{i+1} - \dots - \alpha_n \boldsymbol{x}_n$, $\alpha_i \neq 0 \overset{L3,L6,L9}{\Leftrightarrow} \boldsymbol{x}_i = (\alpha_i^{-1}\alpha_i)\boldsymbol{x}_i = (-\alpha_i^{-1}\alpha_1)\boldsymbol{x}_1 + \dots + (-\alpha_i^{-1}\alpha_{i-1})\boldsymbol{x}_{i-1} + (-\alpha_i^{-1}\alpha_{i+1})\boldsymbol{x}_{i+1} + \dots + (-\alpha_i^{-1}\alpha_n)\boldsymbol{x}_n$ $\Rightarrow$ existuje $\boldsymbol{x}_i =: \boldsymbol{x} \in M$: $\boldsymbol{x} \in \mathcal{L}(M - \{\boldsymbol{x}\})$. Poslední implikaci lze i obrátit, neboť stačí položit $\alpha_i = 1$ (totiž $1 \neq 0$) a užít L4. □

D.21. DŮKAZ věty 3.19:

$\boxed{(1) \Rightarrow (2)}$ G báze ve $V \overset{3.15}{\Rightarrow} G$ je minimální s vlastností $\mathcal{L}(G) = V$. Pak nutně G musí být nezávislá, neboť jinak by dle 3.18 existoval prvek $\boldsymbol{x} \in G$: $\boldsymbol{x} \in \mathcal{L}(G - \{\boldsymbol{x}\}) \overset{3.14(5)}{\Rightarrow} \mathcal{L}(G - \{\boldsymbol{x}\}) = \mathcal{L}(G)$, což je spor s minimalitou G. G je maximální s touto vlastností, neboť každý další prvek $\boldsymbol{x} \in V - G$ leží v $\mathcal{L}(G)$, takže $G \cup \{\boldsymbol{x}\}$ již musí být dle 3.18 lineárně závislá.

$\boxed{(2) \Rightarrow (3)}$ G je dle (2) lineárně nezávislá, zbývá tedy ukázat, že generuje celý prostor. Kdyby tomu tak nebylo, pak $\mathcal{L}(G) \subset V$ a můžeme vybrat nějaký prvek $\boldsymbol{x} \in V - \mathcal{L}(G)$, $\boldsymbol{x} \neq \boldsymbol{0}$, neboť $\boldsymbol{0} \in \mathcal{L}(G)$. Jeho přidáním ke G dostaneme lineárně nezávislou vlastní nadmnožinu $G \cup \{\boldsymbol{x}\} \supset G$, takže G by nebyla maximální taková (spor). K ověření lineární nezávislosti této nadmnožiny stačí ověřit, že každá její neprázdná konečná podmnožina $N \subseteq G \cup \{\boldsymbol{x}\}$ je lineárně nezávislá (srov. 3.16). Mohou nastat dva případy:

a) $\underline{N \subseteq G}$, kdy N musí být nezávislá dle 3.17(1), neboť G je nezávislá;

b) $\underline{\boldsymbol{x} \in N}$, kdy $N =: \{\boldsymbol{x}, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\}$, $\boldsymbol{x}_i \in G$ pro $i = 1, \ldots, k$, $k \geq 0$. Z podmínky $\alpha\boldsymbol{x} + \alpha_1\boldsymbol{x}_1 + \cdots + \alpha_k\boldsymbol{x}_k$ dostáváme $\alpha = 0$. Při $k = 0$ toto plyne z L5, při $k > 0$ analogicky jako v důkazu D.20 předpoklad $\alpha \neq 0$ vede ke sporu $\boldsymbol{x} = (-\alpha^{-1}\alpha_1)\boldsymbol{x}_1 + \cdots + (-\alpha^{-1}\alpha_k)\boldsymbol{x}_k \in \mathcal{L}(G)$. Jelikož $\alpha = 0$, musí být v případě $k > 0$ nulové i ostatní koeficienty α_i pro $i = 1, \ldots, k$, neboť $\boldsymbol{x}_i$ patří do lineárně nezávislé množiny G.

$\boxed{(3) \Rightarrow (1)}$ Dle (3) $\mathcal{L}(G) = V$ platí. Zbývá ukázat, že G je minimální s touto vlastností. Kdyby tomu tak nebylo, pak existuje vlastní podmnožina $G' \subset G$: $\mathcal{L}(G') = V$ a prvek $\boldsymbol{x} \in G - G'$ je lineární kombinací prvků z $G' \subset G \overset{3.18}{\Rightarrow} G$ je lineárně závislá, což je spor s (3). $\square$

D.22. Důkaz důsledku 3.20:

Zvolme nějakou lineárně nezávislou podmnožinu N_0 v G, $\mathcal{L}(N_0) = V$. Alespoň jedna taková existuje: totiž $V \neq \{\boldsymbol{0}\} \Rightarrow G \neq \emptyset$ a existuje $\boldsymbol{0} \neq \boldsymbol{x} \in G$. Dle L5 pak stačí položit $N_0 = \{\boldsymbol{x}\}$. Pokud existuje nějaká vlastní lineárně nezávislá nadmnožina množiny N_0, označme ji N_1, atd. Dostaneme tak konečný nebo nekonečný řetězec lineárně nezávislých množin $N_0 \subset N_1 \subset N_2 \subset \dots$, jehož sjednocením $N = \bigcup_i N_i$ je hledaná maximální lineárně nezávislá množina (tedy báze) obsahující N_0. N je opravdu lineárně nezávislá, neboť každá její neprázdná konečná podmnožina je podmnožinou některé lineárně nezávislé množiny N_i a tudíž lineárně nezávislá dle 3.17(1). Z konstrukce plyne, že N je maximální taková (v opačném případě by musela být nekoncovým prvkem řetězce). $\square$

D.23. <u>DŮKAZ důsledku 3.22</u>:
Podle 3.20 lze z konečného systému generátorů vybrat bázi, která je ovšem také konečná.
Jsou-li ve Steinitzově větě obě množiny M a N bázemi, pak jejich role lze zaměnit:
V N existuje podmnožina N': $\operatorname{card} M = \operatorname{card} N' \leq \operatorname{card} N$ a současně v M existuje podmnožina M': $\operatorname{card} N = \operatorname{card} M' \leq \operatorname{card} M$. Celkem tedy $\operatorname{card} N = \operatorname{card} M$. $\square$

D.24. <u>DŮKAZ důsledku 3.24</u>:
(1) Jestliže $\dim V = \infty$, pak $k \leq \dim V$ platí triviálně.
Pokud $n := \dim V < \infty$, tak ve V existuje báze N o n prvcích a ve větě 3.21 stačí položit $M := \{\boldsymbol{x}_1, \dots, \boldsymbol{x}_k\}$. M má právě k prvků, protože $\boldsymbol{x}_1, \dots, \boldsymbol{x}_k$ musí být navzájem různé, když jsou lineárně nezávislé. Pak $N' \subseteq N$ má tedy také k prvků a tudíž $k \leq n$.
Nerovnost i tvrzení o rozšíření také plyne přímo z věty 3.19(2) nebo jejího důsledku 3.20.
(2) Je-li $V = \{\mathbf{0}\}$, pak bází je prázdná množina. V opačném případě ve V existuje nenulový prvek $\boldsymbol{x}$ a jednoprvková množina $\{\boldsymbol{x}\}$ je dle 3.3(L5) lineárně nezávislá. Podle (1) ji lze doplnit na bázi.
(3) Jestliže $\dim V = \infty$, pak $\dim W \leq \dim V$ platí triviálně, neboť $\dim W = \infty$ nebo $\dim W < \infty$.
Pokud $n := \dim V < \infty$, pak dle 3.19(2) ve V může existovat nejvýše n-prvková lineárně nezávislá podmnožina a tudíž každá báze W může mít nejvýše n prvků. S uvážením 3.22 a 3.23 je tedy $\dim W \leq \dim V$.
Pokud $W \neq V$, pak žádná báze W negeneruje V a nemůže být dle

3.19(2)(3) maximální lineárně nezávislou podmnožinou ve V a tudíž je třeba přidat nejméně jeden prvek, aby jí byla. Pak ovšem nutně $\dim W < \dim V$.

(4) $\boxed{(i) \Rightarrow (ii)}$ G báze $\Rightarrow G$ má n prvků dle 3.22 a 3.23 a je lineárně nezávislá dle 3.19.

$\boxed{(ii) \Rightarrow (iii)}$ Sporem: Kdyby lineárně nezávislá podmnožina o n prvcích negenerovala V, pak dle (1) ji lze na bázi ve V rozšířit přidáním alespoň jednoho prvku, tj. platilo by $\dim V > n$, spor.

$\boxed{(iii) \Rightarrow (i)}$ Sporem: Kdyby n-prvková množina generovala V a nebyla by bází, pak by dle 3.15 nebyla minimální taková, tj.existovala by její vlastní podmnožina rovněž generující V a platilo by tedy $\dim V < n$, spor. $\square$

D.25. DŮKAZ věty 3.27:

$\boxed{\Rightarrow}$ Je-li T lineární zobrazení (tj. homomorfizmus), pak musí zachovávat všechny operace z $\mathcal{L}_{\mathbb{F}}$, tj. zejména také grupové sečítání a násobení skaláry, což jsou právě vlastnosti (1) a (2).

$\boxed{\Leftarrow}$ Má-li T vlastnosti (1) a (2), zbývá ověřit, že má i ty zbývající:

a) $\underline{T \text{ zachovává unární operaci výběru opačného prvku:}}$

$T(-\boldsymbol{x}) \overset{L6}{=} T((-1)\boldsymbol{x}) \overset{(2)}{=} (-1)T(\boldsymbol{x}) \overset{L6}{=} -1 \cdot T(\boldsymbol{x}) \overset{L4}{=} -T(\boldsymbol{x})$.

b) $\underline{T \text{ zachovává nulový prvek:}}$

$T(\mathbf{0}) \overset{L5}{=} T(0 \cdot \boldsymbol{x}) \overset{(2)}{=} 0 \cdot T(\boldsymbol{x}) \overset{L5}{=} \mathbf{0}$.

Je-li T bijekce, pak inverzní zobrazení je homomorfizmus, protože vektorový prostor je strukturou bez relací (viz poznámku 2.61). Složení dvou homomorfizmů dokonce libovolných struktur je vždy homorfizmus (viz dedinici 2.10). V případě vektorových prostorů stačí pro složení dvou lineárních zobrazení $T_1 : V_1 \to V_2$ a $T_2 : V_2 \to V_3$ toto tvrzení snadno ověřit jen pro vlastnosti (1) a (2):

(1) $(T_2T_1)(\boldsymbol{x}+\boldsymbol{y}) = T_2(T_1(\boldsymbol{x}+\boldsymbol{y})) = T_2(T_1(\boldsymbol{x})+T_1(\boldsymbol{y})) = T_2(T_1(\boldsymbol{x}))+ T_2(T_1(\boldsymbol{y})) = (T_2T_1)(\boldsymbol{x}) + (T_2T_1)(\boldsymbol{y})$.

(2) $(T_2T_1)(\alpha\boldsymbol{x}) = T_2(T_1(\alpha\boldsymbol{x})) = T_2(\alpha T_1(\boldsymbol{x})) = \alpha T_2(T_1(\boldsymbol{x})) = \alpha(T_2T_1)(\boldsymbol{x})$.
$\square$

D.26. <u>DŮKAZ důsledku 3.28</u>:
Opakovaným užitím věty 3.27 dostáváme:
$T(\alpha_1\boldsymbol{x}_1 + \cdots + \alpha_n\boldsymbol{x}_n) \overset{(1)}{=} T(\alpha_1\boldsymbol{x}_1) + \cdots + T(\alpha_n\boldsymbol{x}_n) \overset{(2)}{=}$
$\alpha_1 T(\boldsymbol{x}_1) + \cdots + \alpha_n T(\boldsymbol{x}_n)$. $\square$

D.27. <u>DŮKAZ věty 3.29</u>:
Pro obě množiny stačí pomocí věty 3.27 ověřit vlastnosti 3.7(1)(2):
a) <u>pro $\mathcal{N}(T)$</u>:
(1) $\boldsymbol{x}_1, \boldsymbol{x}_2 \in \mathcal{N}(T) \Rightarrow T(\boldsymbol{x}_1) = \boldsymbol{0}$, $T(\boldsymbol{x}_2) = \boldsymbol{0} \Rightarrow T(\boldsymbol{x}_1 + \boldsymbol{x}_2) = T(\boldsymbol{x}_1) + T(\boldsymbol{x}_2) = \boldsymbol{0} + \boldsymbol{0} = \boldsymbol{0} \Rightarrow \boldsymbol{x}_1 + \boldsymbol{x}_2 \in \mathcal{N}(T)$.
(2) $\boldsymbol{x}_1 \in \mathcal{N}(T)$, $\alpha \in \mathbb{F} \Rightarrow T(\boldsymbol{x}_1) = \boldsymbol{0}$ a $T(\alpha\boldsymbol{x}_1) = \alpha T(\boldsymbol{x}_1) = \alpha\boldsymbol{0} \overset{L5}{=} \boldsymbol{0}$ $\Rightarrow \alpha\boldsymbol{x}_1 \in \mathcal{N}(T)$.
b) <u>pro $\mathcal{R}(T)$</u>:
(1) $\boldsymbol{y}_1, \boldsymbol{y}_2 \in \mathcal{R}(T) \Rightarrow \exists\, \boldsymbol{x}_1, \boldsymbol{x}_2 \in V_1 : \boldsymbol{y}_1 = T\boldsymbol{x}_1, \boldsymbol{y}_2 = T\boldsymbol{x}_2 \Rightarrow \boldsymbol{y}_1 + \boldsymbol{y}_2 = T\boldsymbol{x}_1 + T\boldsymbol{x}_2 = T(\boldsymbol{x}_1 + \boldsymbol{x}_2) \Rightarrow \boldsymbol{y}_1 + \boldsymbol{y}_2 \in \mathcal{R}(T)$.
(2) $\boldsymbol{y} \in \mathcal{R}(T)$, $\alpha \in \mathbb{F} \Rightarrow \exists\, \boldsymbol{x} \in V_1 : \boldsymbol{y} = T\boldsymbol{x}$ a $\alpha\boldsymbol{y} = \alpha T\boldsymbol{x} = T(\alpha\boldsymbol{x}) \Rightarrow \alpha\boldsymbol{y} \in \mathcal{R}(T)$. $\square$

D.28. Důkaz důsledku 3.30:
(1) $\boxed{\Rightarrow}$ T izomorfní vnoření $\Rightarrow$ T je prosté $\Rightarrow$ kromě $\boldsymbol{0}$ se žádný jiný prvek ve V_1 nemůže zobrazit na nulový prvek ve $V_2 \Rightarrow \mathcal{N}(T) = \{\boldsymbol{0}\}$.
$\boxed{\Leftarrow}$ Nechť $\mathcal{N}(T) = \{\boldsymbol{0}\}$ a $T\boldsymbol{x} = T\boldsymbol{y}$. Pak $T(\boldsymbol{x} - \boldsymbol{y}) = T\boldsymbol{x} - T\boldsymbol{y} = \boldsymbol{0}$ $\Rightarrow \boldsymbol{x} - \boldsymbol{y} \in \mathcal{N}(T) \Rightarrow \boldsymbol{x} - \boldsymbol{y} = \boldsymbol{0} \Rightarrow \boldsymbol{x} = \boldsymbol{y}$.
(2) T je izomorfizmus $\Leftrightarrow$ T je surjektivní izomorfní vnoření $\overset{(1)}{\Leftrightarrow}$ $\mathcal{N}(T) = \{\boldsymbol{0}\}$ a $\mathcal{R}(T) = V_2$.
(3) $\boxed{\Rightarrow}$ Nechť T je izomorfní vnoření a $E := \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ nějaká neprázdná ($n \in \mathbb{N}$) n-prvková množina, tj. $\boldsymbol{e}_i \neq \boldsymbol{e}_j$ pro $i \neq j$. Protože T je prosté, tak obraz $T(E)$ má tytéž vlastnosti a je tedy také n-prvková. Nechť E je navíc lineárně nezávislá. Pak $\boldsymbol{0} = \alpha_1 T\boldsymbol{e}_1 + \cdots + \alpha_n T\boldsymbol{e}_n \overset{3.28}{=} T(\alpha_1\boldsymbol{e}_1 + \cdots + \alpha_n\boldsymbol{e}_n) \Rightarrow \alpha_1\boldsymbol{e}_1 + \cdots + \alpha_n\boldsymbol{e}_n \in \mathcal{N}(T) \overset{(1)}{=} \{\boldsymbol{0}\} \Rightarrow \alpha_1\boldsymbol{e}_1 + \cdots + \alpha_n\boldsymbol{e}_n = \boldsymbol{0} \Rightarrow \alpha_1 = \cdots = \alpha_n = 0$, neboť prvky E

jsou lineárně nezávislé. Tedy $T(E)$ je rovněž lineárně nezávislá.
$\boxed{\Leftarrow}$ Nechť naopak T zobrazí každou konečnou neprázdnou lineárně nezávislou množinu na lineárně nezávislou množinu s týmž počtem prvků. Podle (1) stačí ukázat, že v takovém případě $\mathcal{N}(T) = \{\mathbf{0}\}$. Pokud $V_1 = \{\mathbf{0}\}$, pak je toto splněno triviálně. V opačném případě ve V_1 existuje alespoň jeden nenulový prvek. Sporem ukážeme, že žádný takový prvek nemůže ležet v $\mathcal{N}(T)$. Kdyby tomu tak bylo, tj. kdyby existoval $\mathbf{0} \neq \boldsymbol{x} \in \mathcal{N}(T)$, pak jednoprvková množina $\{\boldsymbol{x}\}$ by byla dle (L5) lineárně nezávislá a tedy podle předpokládané vlastnosti zobrazení T by musela být lineárně nezávislá také jednoprvková množina $\{T\boldsymbol{x}\}$. Je však $T\boldsymbol{x} = \mathbf{0}$, neboť $\boldsymbol{x} \in \mathcal{N}(T)$ a dostáváme tak spor s 3.17(2).
(4) $\boxed{\Rightarrow}$ Nechť T je izomorfizmus a E libovolná báze ve V_1. Rovnost mohutností $\operatorname{card} T(E) = \operatorname{card} E$ je zřejmá, neboť T je prosté. K tomu, aby $T(E)$ byla báze stačí podle 3.19(3) ukázat, že $T(E)$ je lineárně nezávislá a $\mathcal{L}(T(E)) = V_2$:
a) <u>lineární nezávislost $T(E)$</u>: podle definice 3.16 stačí ukázat, že každá její konečná podmnožina $\emptyset \neq N \subseteq T(E)$ je lineárně nezávislá. To plyne bezprostředně ze (3), protože N je obrazem konečné podmnožiny $T^{-1}(N) \subseteq E$, která je lineárně nezávislá dle 3.17(1).
b) <u>$T(E)$ generuje V_2</u>: Jelikož T je surjektivní, tak každý prvek $\boldsymbol{y} \in V_2$ je obrazem nějakého prvku z $V_1 = \mathcal{L}(E)$, tj. je obrazem nějaké lineární kombinace:
$\boldsymbol{y} = T(\alpha_1\boldsymbol{e}_1 + \cdots + \alpha_n\boldsymbol{e}_n) \overset{3.28}{=} \alpha_1 T\boldsymbol{e}_1 + \cdots + \alpha_n T\boldsymbol{e}_n \in \mathcal{L}(T(E))$.
Tedy $V_2 = \mathcal{L}(T(E))$, což se mělo dokázat.
$\boxed{\Leftarrow}$ Předpokládejme, že T zachovává nějakou bázi E ve V_1 včetně mohutnosti. Je třeba ověřit, že pak T je izomorfizmus, neboli:
a) <u>T je izomorfní vnoření</u>: dle (1) stačí ukázat $\mathcal{N}(T) = \{\mathbf{0}\}$. Podle předpokladu je $T(E)$ báze ve V_2. Nechť $\boldsymbol{x} \in \mathcal{N}(T)$, pak $\boldsymbol{x} = \alpha_1\boldsymbol{e}_1 + \cdots + \alpha_n\boldsymbol{e}_n$, $\boldsymbol{e}_i \in E$ a $\mathbf{0} = T\boldsymbol{x} = T(\alpha_1\boldsymbol{e}_1 + \cdots + \alpha_n\boldsymbol{e}_n) \overset{3.28}{=} \alpha_1 T\boldsymbol{e}_1 + \cdots + \alpha_n T\boldsymbol{e}_n \Rightarrow \alpha_1 = \cdots = \alpha_n = 0$ v důsledku nezávislosti báze $T(E)$ $\Rightarrow \boldsymbol{x} = \mathbf{0}$. Tedy v jádře leží pouze nulový prvek.
a) <u>T je surjekce</u>: buď $\boldsymbol{y} \in V_2$ libovolný. Protože $T(E)$ je báze ve V_2,

tak $\boldsymbol{y} = \alpha_1 T\boldsymbol{e}_1 + \cdots + \alpha_n T\boldsymbol{e}_n \overset{3.28}{=} T(\alpha_1\boldsymbol{e}_1 + \cdots + \alpha_n\boldsymbol{e}_n)$ pro vhodná $\alpha_i \in \mathbb{F}$ a nějaká $\boldsymbol{e}_i \in E$. Tedy T je surjekce. $\square$

D.29. <u>DŮKAZ věty 3.32</u>:
Dle 3.30(2) stačí ověřit $\mathcal{N}([\cdot]_E) = \{\mathbf{0}\}$ a $\mathcal{R}([\cdot]_E) = \mathbb{F}^n$:
• $\boldsymbol{x} \in \mathcal{N}([\cdot]_E) \Rightarrow [\boldsymbol{x}]_E = [\mathbf{0}, \ldots, \mathbf{0}] \Rightarrow \boldsymbol{x} = 0 \cdot \boldsymbol{e}_1 + \cdots + 0 \cdot \boldsymbol{e}_n = \mathbf{0} \Rightarrow \mathcal{N}([\cdot]_E) = \{\mathbf{0}\}$.
• Buď $[\xi_1, \ldots, \xi_n] \in \mathbb{F}^n$ libovolná n-tice, pak
$\boldsymbol{x} := \xi_1\boldsymbol{e}_1 + \cdots + \xi_n\boldsymbol{e}_n \in \mathcal{L}(E) = V \Rightarrow [\boldsymbol{x}]_E = [\xi_1, \ldots, \xi_n]$. Tedy každá n-tice je obrazem nějakého vektoru z V, takže $[\cdot]_E$ je surjekce. $\square$

D.30. <u>DŮKAZ důsledku 3.33</u>:
(1) $\boxed{\Rightarrow}$ Nechť $\dim V_1 = \dim V_2 =: n$ a E_1 a E_2 jsou nějaké n-prvkové báze pořadě ve V_1 a V_2. Pak dle 3.32 V_1 i V_2 jsou izomorfní s $\mathbb{F}^n$, takže jsou nutně izomorfní navzájem: stačí složit izomorfizmy
$V_1 \xrightarrow{[\cdot]_{E_1}} \mathbb{F}^n \xrightarrow{[\cdot]_{E_2}^{-1}} V_2$.
$\boxed{\Leftarrow}$ Je-li $T : (V_1, \mathcal{L}_\mathbb{F}) \to (V_2, \mathcal{L}_\mathbb{F})$ izomorfizmus a E_1 nějaká n-prvková báze ve V_1 pak $T(E_1)$ je dle 3.30(4) rovněž n-prvková báze ve V_2 a tudíž $\dim V_1 = \dim V_2 = n$.
(2) $\boxed{\Rightarrow}$ Nechť $n := \dim V_1 \leq \dim V_2 =: m$ a E_1 je nějaká n-prvková báze ve V_1 a E_2 m-prvková báze ve V_2. Libovolných n prvků vybraných z E_2 generuje ve V_2 podprostor dimenze n (viz 3.24(4)), který je dle (1) izomorfní s V_1, takže V_1 lze izomorfně vnořit do V_2.
$\boxed{\Leftarrow}$ Je-li naopak $T : V_1 \to V_2$ nějaké izomorfní vnoření, pak $\mathcal{R}(T)$ je podprostor ve V_2 (viz 3.29) izomorfní s V_1 a opět dle (1) dostáváme $\dim V_1 = \dim \mathcal{R}(T) \leq \dim V_2$ s uvážením 3.24(3). $\square$

D.31. DŮKAZ věty 3.36:
Tato věta je shrnutím některých předchozích výsledků:
(1) $\mathcal{R}(T) = \{T\boldsymbol{x} \mid \boldsymbol{x} \in V_1 = \mathcal{L}(E_1)\} \overset{3.12(2)}{=}$
$\{T(\sum_{i=1}^n \xi_i\boldsymbol{e}_i) \mid \xi_i \in \mathbb{F}, \boldsymbol{e}_i \in E_1, i = 1, \ldots, n; n \in \mathbb{N}\} \overset{3.28}{=}$
$\{\sum_{i=1}^n \xi_i T(\boldsymbol{e}_i) \mid \xi_i \in \mathbb{F}, T(\boldsymbol{e}_i) \in T(E_1), i = 1, \ldots, n; n \in \mathbb{N}\} \overset{3.12(2)}{=}$
$\mathcal{L}(T(E_1))$.

(2) $\mathcal{L}(T(E_1)) = V_2 \overset{(1)}{\Leftrightarrow} \mathcal{R}(T) = V_2 \ \Leftrightarrow \ T$ je surjekce.
(3) $T : V_1 \to V_2$ izomorfní vnoření $\Rightarrow T : V_1 \to \mathcal{R}(T)$ je izomorfizmus. Pak $T(E_1)$ je báze v $\mathcal{R}(T)$ pro každou bázi E_1 ve V_1 dle 3.30(4).

(4) E_1 báze ve $V_1 \overset{3.19}{\Rightarrow} E_1$ je lineárně nezávislá ve $V_1 \overset{3.30(3)}{\Rightarrow} T(E_1)$ je lineárně nezávislá ve V_2.
(5) Jedná se přímo o tvrzení 3.30(4). Je také důsledkem (3) uvážíme-li, že v případě izomorfizmu je $\mathcal{R}(T) = V_2$.
(6) Nechť $f : E_1 \to V_2$ je libovolné zobrazení. Podle poznámky 3.34 hledaný operátor T je pro libovolné $\boldsymbol{x} \in V_1$ jednoznačně určen vztahem $T\boldsymbol{x} := \xi_1 f(\boldsymbol{e}_1) + \cdots + \xi_n f(\boldsymbol{e}_n)$, kde $\boldsymbol{x} = \xi_1 \boldsymbol{e}_1 + \cdots + \xi_n \boldsymbol{e}_n$ je vyjádření vektoru $\boldsymbol{x}$ pomocí vhodných bázových prvků $\boldsymbol{e}_i \in E_1$. Protože E_1 je jakožto báze lineárně nezávislá množina (viz 3.19) je dle 3.17(4) až na případné nulové koeficienty toto vyjádření jediné, takže T je korektně definováno. Zřejmě restrikce T na E_1 je právě f, neboť $T\boldsymbol{e} = T(1 \cdot \boldsymbol{e}) = 1 \cdot f(\boldsymbol{e}) = f(\boldsymbol{e})$ pro každé $\boldsymbol{e} \in E_1$. Zbývá ověřit, že takto zavedené zobrazení je lineární, tj. ověřit vlastnosti 3.27(1)(2). Jejich platnost je však bezprostředním důsledkem elementárních vlastností (L3) a (L11):
• $\alpha\boldsymbol{x} = \alpha(\xi_1 \boldsymbol{e}_1 + \cdots + \xi_n \boldsymbol{e}_n) = (\alpha\xi_1)\boldsymbol{e}_1 + \cdots + (\alpha\xi_n)\boldsymbol{e}_n \Rightarrow T(\alpha\boldsymbol{x}) = (\alpha\xi_1) f(\boldsymbol{e}_1) + \cdots + (\alpha\xi_n) f(\boldsymbol{e}_n) = \alpha(\xi_1 f(\boldsymbol{e}_1) + \cdots + \xi_n f(\boldsymbol{e}_n)) = \alpha T(\boldsymbol{x})$.
• Podobně pro sečítání. Nechť $\boldsymbol{y} = \eta_1 \boldsymbol{e}_1 + \cdots + \eta_n \boldsymbol{e}_n$ je další vektor, kde $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ jsme zvolili jako sjednocení bázových vektorů z vyjádření pro $\boldsymbol{x}$ a $\boldsymbol{y}$ vhodným doplněním nulových koeficientů ξ_k a η_j. Pak $\boldsymbol{x} + \boldsymbol{y} = (\xi_1 \boldsymbol{e}_1 + \cdots + \xi_n \boldsymbol{e}_n) + (\eta_1 \boldsymbol{e}_1 + \cdots + \eta_n \boldsymbol{e}_n) = (\xi_1 + \eta_1)\boldsymbol{e}_1 + \cdots + (\xi_n + \eta_n)\boldsymbol{e}_n \Rightarrow T(\boldsymbol{x} + \boldsymbol{y}) = (\xi_1 + \eta_1) f(\boldsymbol{e}_1) + \cdots + (\xi_n + \eta_n) f(\boldsymbol{e}_n) = (\xi_1 f(\boldsymbol{e}_1) + \cdots + \xi_n f(\boldsymbol{e}_n)) + (\eta_1 f(\boldsymbol{e}_1) + \cdots + \eta_n f(\boldsymbol{e}_n)) = T\boldsymbol{x} + T\boldsymbol{y}$.
• Nechť navíc f (a tedy i T) je prosté zobrazení do nějaké báze E_2, resp. bijekce na E_2. Pak $f(E_1)$ je s uvážením 3.17(1) lineárně nezávislá podmnožina v E_2 téže mohutnosti generující $\mathcal{R}(T)$: to plyne z 3.12(2), neboť dle konstrukce T prvky z $\mathcal{R}(T)$ jsou právě všechny lineární kombinace prvků z $f(E_1)$. Obraz $f(E_1)$ je tedy dle 3.19(3) báze v $\mathcal{R}(T)$ a podle 3.30(4) je pak T izomorfizmus V_1 na $\mathcal{R}(T)$, a tudíž

izomorfní vnoření V_1 do V_2. Je-li f dokonce bijekce, pak $f(E_1) = E_2$ je báze ve V_2, takže $\mathcal{R}(T) = V_2$ a T je tedy izomorfizmus. $\square$

D.32. <u>DŮKAZ věty 3.55</u>:
Pro libovolné $\boldsymbol{x}, \boldsymbol{y} \in V$ dostáváme:
$\boldsymbol{x} = (\boldsymbol{x}-\boldsymbol{y}) + \boldsymbol{y} \overset{N1}{\Rightarrow} \|\boldsymbol{x}\| \leq \|\boldsymbol{x}-\boldsymbol{y}\| + \|\boldsymbol{y}\| \Rightarrow \underline{\|\boldsymbol{x}\| - \|\boldsymbol{y}\| \leq \|\boldsymbol{x}-\boldsymbol{y}\|}$.
Analogicky záměnou role $\boldsymbol{x}$ a $\boldsymbol{y}$:
$\underline{-(\|\boldsymbol{x}\| - \|\boldsymbol{y}\|)} = \|\boldsymbol{y}\| - \|\boldsymbol{x}\| \leq \|\boldsymbol{y}-\boldsymbol{x}\| = \|(-1)(\boldsymbol{x}-\boldsymbol{y})\| \overset{N2}{=} \underline{\|\boldsymbol{x}-\boldsymbol{y}\|}$.
Protože absolutní hodnota rozdílu se od něj liší pouze znaménkem, dostáváme z obou podtržených nerovností:
$|\|\boldsymbol{x}\| - \|\boldsymbol{y}\|| \leq \|\boldsymbol{x}-\boldsymbol{y}\|$. Dosazením $-\boldsymbol{y}$ místo $\boldsymbol{y}$, pak $\|\pm\boldsymbol{y}\| \overset{N2}{=} \|\boldsymbol{y}\|$ a platí tedy i obdobná nerovnost pro normu součtu:
$|\|\boldsymbol{x}\| - \|\boldsymbol{y}\|| = |\|\boldsymbol{x}\| - \|-\boldsymbol{y}\|| \leq \|\boldsymbol{x} - (-\boldsymbol{y})\| = \|\boldsymbol{x}+\boldsymbol{y}\|$. Dokázali jsme tak levou z obou nerovností.
Pravá nerovnost je vlastně přímo trojúhelníková nerovnost (N1):
$\|\boldsymbol{x} \pm \boldsymbol{y}\| \leq \|\boldsymbol{x}\| + \|\pm\boldsymbol{y}\| \overset{N2}{=} \|\boldsymbol{x}\| + \|\boldsymbol{y}\|$. $\square$

D.33. <u>DŮKAZ věty 3.59</u>:
(S5) $\langle \boldsymbol{x}, \boldsymbol{y}+\boldsymbol{z}\rangle \overset{S3}{=} \overline{\langle \boldsymbol{y}+\boldsymbol{z}, \boldsymbol{x}\rangle} \overset{S1}{=} \overline{\langle \boldsymbol{y}, \boldsymbol{x}\rangle + \langle \boldsymbol{z}, \boldsymbol{x}\rangle} = \overline{\langle \boldsymbol{y}, \boldsymbol{x}\rangle} + \overline{\langle \boldsymbol{z}, \boldsymbol{x}\rangle} \overset{S3}{=} \langle \boldsymbol{x}, \boldsymbol{y}\rangle + \langle \boldsymbol{x}, \boldsymbol{z}\rangle$.
(S6) $\langle \boldsymbol{x}, \alpha\boldsymbol{y}\rangle \overset{S3}{=} \overline{\langle \alpha\boldsymbol{y}, \boldsymbol{x}\rangle} \overset{S2}{=} \overline{\alpha\langle \boldsymbol{y}, \boldsymbol{x}\rangle} = \overline{\alpha}\overline{\langle \boldsymbol{y}, \boldsymbol{x}\rangle} \overset{S3}{=} \overline{\alpha}\langle \boldsymbol{x}, \boldsymbol{y}\rangle$.
(S7) $\langle \boldsymbol{0}, \boldsymbol{x}\rangle \overset{L5}{=} \langle 0 \cdot \boldsymbol{x}, \boldsymbol{x}\rangle \overset{S2}{=} 0 \cdot \langle \boldsymbol{x}, \boldsymbol{x}\rangle = 0$; $\langle \boldsymbol{x}, \boldsymbol{0}\rangle \overset{S3}{=} \overline{\langle \boldsymbol{0}, \boldsymbol{x}\rangle} = \overline{0} = 0$. $\square$

D.34. Důkaz věty 3.61:
Ve speciálním případě $\mathbb{F} = \mathbb{R}$ existuje jednodušší důkaz, který lze nalézt v `[KaSk:V11.5 s.105]`. Zde uvedeme obecný důkaz platný i pro $\mathbb{F} = \mathbb{C}$.
Pro $\boldsymbol{x}, \boldsymbol{y} \in V$; $\alpha, \beta \in \mathbb{F}$ libovolné užitím (S1) až (S6) dostáváme následující úpravu jakožto speciální případ vztahu (3.1):

$$0 \overset{S4}{\leq} \langle \alpha\boldsymbol{x}+\beta\boldsymbol{y}, \alpha\boldsymbol{x}+\beta\boldsymbol{y}\rangle = \alpha\overline{\alpha}\langle \boldsymbol{x}, \boldsymbol{x}\rangle + \alpha\overline{\beta}\langle \boldsymbol{x}, \boldsymbol{y}\rangle + \beta\overline{\alpha}\langle \boldsymbol{y}, \boldsymbol{x}\rangle + \beta\overline{\beta}\langle \boldsymbol{y}, \boldsymbol{y}\rangle.$$

Hlavní myšlenka důkazu spočívá ve vhodné volbě α, β tak, aby nerovnost přešla na tvar kvadratické nerovnosti $At^2 + 2Bt + C \geq 0$, kde

$t, A, B, C \in \mathbb{R}$. Položíme $\alpha := t \in R$ a $\beta := \begin{cases} 1 & \text{pro } \langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0, \\ \frac{\langle \boldsymbol{x}, \boldsymbol{y} \rangle}{|\langle \boldsymbol{x}, \boldsymbol{y} \rangle|} & \text{pro } \langle \boldsymbol{x}, \boldsymbol{y} \rangle \neq 0. \end{cases}$

Pak zřejmě platí $\beta\overline{\beta} = |\beta|^2 = 1$ a v případě $\langle \boldsymbol{x}, \boldsymbol{y} \rangle \neq 0$ máme:

$$\boxed{\overline{\beta}\langle \boldsymbol{x}, \boldsymbol{y} \rangle} = \frac{\overline{\langle \boldsymbol{x}, \boldsymbol{y} \rangle}\langle \boldsymbol{x}, \boldsymbol{y} \rangle}{|\langle \boldsymbol{x}, \boldsymbol{y} \rangle|} = \frac{|\langle \boldsymbol{x}, \boldsymbol{y} \rangle|^2}{|\langle \boldsymbol{x}, \boldsymbol{y} \rangle|} = \boxed{|\langle \boldsymbol{x}, \boldsymbol{y} \rangle|} =$$
$$= \overline{|\langle \boldsymbol{x}, \boldsymbol{y} \rangle|} = \overline{\overline{\beta}\langle \boldsymbol{x}, \boldsymbol{y} \rangle} = \beta\overline{\langle \boldsymbol{x}, \boldsymbol{y} \rangle} \overset{S3}{=} \boxed{\beta\langle \boldsymbol{y}, \boldsymbol{x} \rangle}.$$

Poznamenejme, že rovnost zarámovaných výrazů je zřejmě triviálně splněna i pro druhý případ $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0$. Jelikož $\alpha = t$ je reálné číslo, tak $\alpha = \overline{\alpha} = t$ a po dosazení do výše uvedené nerovnosti tato přejde do požadovaného tvaru:

$$\underbrace{\langle \boldsymbol{x}, \boldsymbol{x} \rangle}_{=:A} t^2 + 2\underbrace{|\langle \boldsymbol{x}, \boldsymbol{y} \rangle|}_{=:B} t + \underbrace{\langle \boldsymbol{y}, \boldsymbol{y} \rangle}_{=:C} \geq 0.$$

Tato kvadratická nerovnost platí pro libovolné $t \in \mathbb{R}$, takže příslušná kvadratická rovnice může mít nejvýše jeden reálný kořen, což nastane právě tehdy, když její diskriminant není kladný, tj. právě když $|\langle \boldsymbol{x}, \boldsymbol{y} \rangle|^2 - \langle \boldsymbol{x}, \boldsymbol{x} \rangle\langle \boldsymbol{y}, \boldsymbol{y} \rangle \leq 0$, tj. právě když $|\langle \boldsymbol{x}, \boldsymbol{y} \rangle|^2 \leq \langle \boldsymbol{x}, \boldsymbol{x} \rangle\langle \boldsymbol{y}, \boldsymbol{y} \rangle$, což již po odmocnění dává dokazovanou nerovnost (S8).
Zbývá už jen ověřit, kdy nastane rovnost. Pokud $\boldsymbol{x}, \boldsymbol{y}$ jsou lineárně závislé, například $\boldsymbol{y} = a\boldsymbol{x}$, pak $|\langle \boldsymbol{x}, \boldsymbol{y} \rangle| = |\langle \boldsymbol{x}, a\boldsymbol{x} \rangle| = |\overline{a}\langle \boldsymbol{x}, \boldsymbol{x} \rangle| = |\overline{a}|\, \|\boldsymbol{x}\|^2 = |a|\, \|\boldsymbol{x}\|\, \|\boldsymbol{x}\| = \|x\|\, \|a\boldsymbol{x}\| = \|\boldsymbol{x}\|\, \|\boldsymbol{y}\|$ a rovnost platí.
Nechť naopak platí rovnost. Pak mohou nastat dvě situace:
a) $\underline{\boldsymbol{x} = \boldsymbol{0} \text{ nebo } \boldsymbol{y} = \boldsymbol{0}}$, kdy $\boldsymbol{x} = 0 \cdot \boldsymbol{y}$ nebo $\boldsymbol{y} = 0 \cdot \boldsymbol{x}$ a $\boldsymbol{x}, \boldsymbol{y}$ jsou tedy lineárně závislé (viz též 3.17(2));
b) $\underline{\boldsymbol{x} \neq \boldsymbol{0} \text{ a } \boldsymbol{y} \neq \boldsymbol{0}}$. Nastane-li rovnost v (S8), pak při popsané volbě α, β to znamená, že platí rovnost i ve výchozí nerovnosti, tj.
$0 = \langle \alpha\boldsymbol{x} + \beta\boldsymbol{y}, \alpha\boldsymbol{x} + \beta\boldsymbol{y} \rangle \overset{S4}{\Rightarrow} \alpha\boldsymbol{x} + \beta\boldsymbol{y} = \boldsymbol{0}$ při $\alpha = t$ a $|\beta|^2 = 1$, tj. zejména $\beta \neq 0$ a $\boldsymbol{x}, \boldsymbol{y}$ jsou tedy lineárně závislé. $\square$

D.35. DŮKAZ důsledku 3.62:
Pro $\|\boldsymbol{x}\| := \sqrt{\langle \boldsymbol{x}, \boldsymbol{x} \rangle}$ ověříme platnost axiomů (N1)–(N3).
(N1) $\|\boldsymbol{x}+\boldsymbol{y}\|^2 \overset{S9}{=} \langle \boldsymbol{x}+\boldsymbol{y}, \boldsymbol{x}+\boldsymbol{y} \rangle \overset{(3.1)}{=} \langle \boldsymbol{x}, \boldsymbol{x} \rangle + \langle \boldsymbol{x}, \boldsymbol{y} \rangle + \langle \boldsymbol{y}, \boldsymbol{x} \rangle + \langle \boldsymbol{y}, \boldsymbol{y} \rangle \overset{S3}{=}$ $\langle \boldsymbol{x}, \boldsymbol{x} \rangle + \langle \boldsymbol{x}, \boldsymbol{y} \rangle + \overline{\langle \boldsymbol{x}, \boldsymbol{y} \rangle} + \langle \boldsymbol{y}, \boldsymbol{y} \rangle = \langle \boldsymbol{x}, \boldsymbol{x} \rangle + 2\mathrm{Re}\, \langle \boldsymbol{x}, \boldsymbol{y} \rangle + \langle \boldsymbol{y}, \boldsymbol{y} \rangle \leq$ $\langle \boldsymbol{x}, \boldsymbol{x} \rangle + 2|\langle \boldsymbol{x}, \boldsymbol{y} \rangle| + \langle \boldsymbol{y}, \boldsymbol{y} \rangle \overset{S8,S9}{\leq} \|\boldsymbol{x}\|^2 + 2\|\boldsymbol{x}\|\|\boldsymbol{y}\| + \|\boldsymbol{y}\|^2 = (\|\boldsymbol{x}\| + \|\boldsymbol{y}\|)^2$ $\Rightarrow \|\boldsymbol{x}+\boldsymbol{y}\| \leq \|\boldsymbol{x}\| + \|\boldsymbol{y}\|$.
(N2) $\|\alpha \boldsymbol{x}\| = \sqrt{\langle \alpha \boldsymbol{x}, \alpha \boldsymbol{x} \rangle} \overset{S2,S6}{=} \sqrt{\alpha\overline{\alpha}\langle \boldsymbol{x}, \boldsymbol{x} \rangle} \overset{S9}{=} \sqrt{|\alpha|^2 \|\boldsymbol{x}\|^2} = |\alpha|\, \|\boldsymbol{x}\|$.
(N3) $\|\boldsymbol{x}\| = 0 \;\Leftrightarrow\; \sqrt{\langle \boldsymbol{x}, \boldsymbol{x} \rangle} = 0 \;\Leftrightarrow\; \langle \boldsymbol{x}, \boldsymbol{x} \rangle = 0 \overset{S4}{\Leftrightarrow} \boldsymbol{x} = 0$. □

D.36. Důkaz věty 3.63:
$\boxed{\Rightarrow}$ Je-li V VS-prostor, pak podobně jako při ověřování axiomu (N1) v předchozím důkazu dostáváme: $\|\boldsymbol{x}+\boldsymbol{y}\|^2 + \|\boldsymbol{x}-\boldsymbol{y}\|^2 =$ $(\|\boldsymbol{x}\|^2 + \langle \boldsymbol{x}, \boldsymbol{y} \rangle + \langle \boldsymbol{y}, \boldsymbol{x} \rangle + \|\boldsymbol{y}\|^2) + (\|\boldsymbol{x}\|^2 - \langle \boldsymbol{x}, \boldsymbol{y} \rangle - \langle \boldsymbol{y}, \boldsymbol{x} \rangle + \|-\boldsymbol{y}\|^2) =$ $2(\|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2)$.
$\boxed{\Leftarrow}$ Platí-li v NL-prostoru (S10), zavedeme v něm skalární součin následovně pomocí tzv. *polarizační identity*:

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle := \begin{cases} \frac{1}{4}\{\|\boldsymbol{x}+\boldsymbol{y}\|^2 - \|\boldsymbol{x}-\boldsymbol{y}\|^2\} & \text{pro } \mathbb{F} = \mathbb{R} \\ \frac{1}{4}\{\|\boldsymbol{x}+\boldsymbol{y}\|^2 - \|\boldsymbol{x}-\boldsymbol{y}\|^2 + & \\ \quad +i(\|\boldsymbol{x}+i\boldsymbol{y}\|^2 - \|\boldsymbol{x}-i\boldsymbol{y}\|^2)\} & \text{pro } \mathbb{F} = \mathbb{C}. \end{cases}$$

Ověření axiomů (S3) a (S4) je snadné zatímco (S1) a (S2) vyžadují poněkud větší úsilí. □

D.37. DŮKAZ věty 3.66:
(a) $\langle \alpha_i \boldsymbol{e}_1, \alpha_j \boldsymbol{e}_j \rangle = \alpha_i \overline{\alpha_j} \langle \boldsymbol{e}_i, \boldsymbol{e}_j \rangle = 0$ pro libovolné $i, j \in \{1, \ldots, n\}$, $i \neq j$, neboť $\langle \boldsymbol{e}_i, \boldsymbol{e}_j \rangle = 0$ v důsledku ortogonality $\boldsymbol{e}_i \perp \boldsymbol{e}_j$.
(b) $\boldsymbol{e}_i \neq \boldsymbol{0}\ \forall i = 1, \ldots, n \overset{N3}{\Rightarrow} \|\boldsymbol{e}_i\| \neq 0\ \forall i = 1, \ldots, n$ a $\{\frac{1}{\|\boldsymbol{e}_i\|}\boldsymbol{e}_i\}$ je ortogonální dle (a), přičemž $\|\frac{1}{\|\boldsymbol{e}_i\|}\boldsymbol{e}_i\| \overset{N2}{=} \frac{1}{\|\boldsymbol{e}_i\|}\|\boldsymbol{e}_i\| = 1$, takže je celkem ortonormální. □

D.38. <u>DŮKAZ věty 3.67</u>:
$\boldsymbol{x} \perp \boldsymbol{y} \Rightarrow \langle \boldsymbol{x}, \boldsymbol{y} \rangle = \langle \boldsymbol{y}, \boldsymbol{x} \rangle = 0 \Rightarrow \|\boldsymbol{x}+\boldsymbol{y}\|^2 = \langle \boldsymbol{x}+\boldsymbol{y}, \boldsymbol{x}+\boldsymbol{y} \rangle = \langle \boldsymbol{x}, \boldsymbol{x} \rangle + \langle \boldsymbol{x}, \boldsymbol{y} \rangle + \langle \boldsymbol{y}, \boldsymbol{x} \rangle + \langle \boldsymbol{y}, \boldsymbol{y} \rangle = \langle \boldsymbol{x}, \boldsymbol{x} \rangle + \langle \boldsymbol{y}, \boldsymbol{y} \rangle = \|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2$. □

D.39. <u>DŮKAZ věty 3.68</u>:
Nechť $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\} \subseteq E$ je libovolná konečná podmnožina. Jelikož E je ortogonální s nenulovými prvky, tak $\langle \boldsymbol{e}_i, \boldsymbol{e}_j \rangle = 0 \; \forall\, i, j \in \{1, \ldots, n\}$, $i \neq j$ a $\langle \boldsymbol{e}_j, \boldsymbol{e}_j \rangle \neq 0$ dle (S4). Pak
$\sum_{i=1}^n \alpha_i \boldsymbol{e}_i = 0 \Rightarrow$ pro libovolné $j \in \{1, \ldots, n\}$ dostáváme $0 \overset{S7}{=} \langle 0, \boldsymbol{e}_j \rangle = \langle \sum_{i=1}^n \alpha_i \boldsymbol{e}_i, \boldsymbol{e}_j \rangle = \sum_{i=1}^n \alpha_i \langle \boldsymbol{e}_i, \boldsymbol{e}_j \rangle = \alpha_j \langle \boldsymbol{e}_j, \boldsymbol{e}_j \rangle \Rightarrow \alpha_j = 0$ pro každé $j = 1, \ldots, n$, neboť $\langle \boldsymbol{e}_j, \boldsymbol{e}_j \rangle \neq 0$. Tedy $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ jsou lineárně nezávislé a E rovněž dle definice 3.16, neboť výběr konečné podmnožiny byl libovolný. □

D.40. <u>DŮKAZ důsledku 3.69</u>:
E báze ve $V \Rightarrow$ pro každé $\boldsymbol{x} \in V$ existují $\xi_i \in \mathbb{F}, \boldsymbol{e}_i \in E$, $i = 1, \ldots, n$ taková, že $\boldsymbol{x} = \sum_{i=1}^n \xi_i \boldsymbol{e}_i \Rightarrow \langle \boldsymbol{x}, \boldsymbol{e}_j \rangle = \langle \sum_{i=1}^n \xi_i \boldsymbol{e}_i, \boldsymbol{e}_j \rangle = \sum_{i=1}^n \xi_i \langle \boldsymbol{e}_i, \boldsymbol{e}_j \rangle = \xi_j \langle \boldsymbol{e}_j, \boldsymbol{e}_j \rangle = \xi_j \|\boldsymbol{e}_j\|^2 = \xi_j$ pro každé $j = 1, \ldots, n$ vzhledem k ortonormalitě E. Toto vyjádření je přitom jediné možné dle 3.17(4). □

D.41. <u>DŮKAZ důsledku 3.70</u>:
Dle 3.69 můžeme po případném doplnění nulových koeficientů zapsat $\boldsymbol{x}$ i $\boldsymbol{y}$ jako lineární kombinaci týchž vektorů:
$\boldsymbol{x} = \sum_{i=1}^n \xi_i \boldsymbol{e}_i$ a $\boldsymbol{y} = \sum_{j=1}^n \eta_j \boldsymbol{e}_j$, kde $\boldsymbol{e}_i \in E$ pro $i = 1, \ldots, n$. Pak
$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \langle \sum_{i=1}^n \xi_i \boldsymbol{e}_i, \sum_{j=1}^n \eta_j \boldsymbol{e}_j \rangle \overset{(3.1)}{=} \sum_{i,j=1}^n \xi_i \overline{\eta}_j \langle \boldsymbol{e}_i, \boldsymbol{e}_j \rangle = \sum_{i=1}^n \xi_i \overline{\eta}_i$.
$\boldsymbol{x} = \boldsymbol{y} \Rightarrow \|x\| = \sqrt{\langle \boldsymbol{x}, \boldsymbol{x} \rangle} = \sqrt{\sum_{i=1}^n \xi_i \overline{\xi}_i} = \sqrt{\sum_{i=1}^n |\xi_i|^2}$. Vztahy pro souřadnice $\xi_i = \langle \boldsymbol{x}, \boldsymbol{e}_i \rangle$ a $\eta_j = \langle \boldsymbol{y}, \boldsymbol{e}_j \rangle$ dostáváme z 3.69. □

D.42. Důkaz věty 3.71:
a) <u>$M^\perp$ je podprostor</u>: dle 3.7 stačí ukázat uzavřenost $M^\perp$ vzhledem k sčítání a násobení skaláry: $\boldsymbol{x}_1, \boldsymbol{x}_2 \in M^\perp \Rightarrow \langle \boldsymbol{x}_1, \boldsymbol{y} \rangle = 0$, $\langle \boldsymbol{x}_2, \boldsymbol{y} \rangle = 0$ pro každé $\boldsymbol{y} \in M \Rightarrow \langle \boldsymbol{x}_1 + \boldsymbol{x}_2, \boldsymbol{y} \rangle \overset{S2}{=} \langle \boldsymbol{x}_1, \boldsymbol{y} \rangle + \langle \boldsymbol{x}_2, \boldsymbol{y} \rangle = 0 + 0 = 0$ pro každé $\boldsymbol{y} \in M \Rightarrow \boldsymbol{x}_1 + \boldsymbol{x}_2 \in M^\perp$.

$\boldsymbol{x} \in M^\perp \Rightarrow \langle \boldsymbol{x}, \boldsymbol{y}\rangle = 0$ pro každé $\boldsymbol{y} \in M \Rightarrow \langle \alpha\boldsymbol{x}, \boldsymbol{y}\rangle \overset{S2}{=} \alpha\langle \boldsymbol{x}, \boldsymbol{y}\rangle = \alpha \cdot 0 = 0$ pro každé $\boldsymbol{y} \in M$ a $\alpha \in \mathbb{F} \Rightarrow \alpha\boldsymbol{x} \in M^\perp$.

b) $\underline{\mathcal{L}(M)^\perp \subseteq M^\perp}$: $\boldsymbol{x} \in \mathcal{L}(M)^\perp \Rightarrow \boldsymbol{x} \perp \boldsymbol{y}$ pro každé $\boldsymbol{y} \in \mathcal{L}(M) \Rightarrow \boldsymbol{x} \perp \boldsymbol{y}$ pro každé $\boldsymbol{y} \in M \subseteq \mathcal{L}(M) \Rightarrow \boldsymbol{x} \in M^\perp$.

c) $\underline{M^\perp \subseteq \mathcal{L}(M)^\perp}$: $\boldsymbol{x} \in M^\perp \Rightarrow \boldsymbol{x} \perp M$. Buď $\boldsymbol{y} \in \mathcal{L}(M)$ libovolný, pak existují $\eta_i \in \mathbb{F}$ a $\boldsymbol{y}_i \in M, i = 1, \ldots, n$: $\boldsymbol{y} = \sum_{i=1}^n \eta_i \boldsymbol{y}_i$ a $\langle \boldsymbol{x}, \boldsymbol{y}\rangle = \langle \boldsymbol{x}, \sum_{i=1}^n \eta_i \boldsymbol{y}_i\rangle \overset{(3.1)}{=} \sum_{i=1}^n \overline{\eta}_i \underbrace{\langle \boldsymbol{x}, \boldsymbol{y}_i\rangle}_{=0} = 0$. Tedy $\boldsymbol{x} \in \mathcal{L}(M)^\perp$.

d) $\underline{M \subseteq N \Rightarrow N^\perp \subseteq M^\perp}$: zřejmé neboť každý prvek kolmý na N musí být též kolmý na M, když platí $M \subseteq N$. $\square$

D.43. DŮKAZ věty 3.73:

Pro každé $i \in I$ platí: $W_i \perp W_j$ pro $i \neq j \Rightarrow W_i \perp \bigcup_{j\neq i} W_j \overset{3.71,3.72}{\Rightarrow} W_i \perp \mathcal{L}(\bigcup_{j\neq i} W_j)$. Pokud $\boldsymbol{x} \in W_i \cap \mathcal{L}(\bigcup_{j\neq i} W_j)$, pak $\boldsymbol{x} \perp \boldsymbol{x} \Rightarrow 0 = \langle \boldsymbol{x}, \boldsymbol{x}\rangle \overset{S4}{\Rightarrow} \boldsymbol{x} = \boldsymbol{0}$. Tedy $W_i \cap \mathcal{L}(\bigcup_{j\neq i} W_j) = \{\boldsymbol{0}\}$ pro každé $i \in I$ a tudíž součet $W = \sum_{i\in I} W_i$ je přímý podle definice 3.43. $\square$

D.44. DŮKAZ věty 3.74:

Nechť W' je nějaký přímý doplněk ortogonální k W, pak samozřejmě $W' \subseteq W^\perp$. Zbývá ukázat i opačnou inkluzi. Nechť tedy naopak $\boldsymbol{x} \in W^\perp$ je libovolný prvek, pak $\boldsymbol{x} = \boldsymbol{w} + \boldsymbol{w}'$, kde $\boldsymbol{w} \in W$ a $\boldsymbol{w}' \in W'$, přičemž $0 = \langle \boldsymbol{x}, \boldsymbol{w}\rangle = \langle \boldsymbol{w} + \boldsymbol{w}', \boldsymbol{w}\rangle \overset{S1}{=} \langle \boldsymbol{w}, \boldsymbol{w}\rangle + \underbrace{\langle \boldsymbol{w}', \boldsymbol{w}\rangle}_{=0} = \langle \boldsymbol{w}, \boldsymbol{w}\rangle \overset{S4}{\Rightarrow} \boldsymbol{w} = \boldsymbol{0} \Rightarrow \boldsymbol{x} = \boldsymbol{w}' \in W'$. Platí tedy také $W^\perp \subseteq W'$ a tedy celkem $W^\perp = W'$. $\square$

D.45. DŮKAZ důsledku 3.75:

Plyne ze symetrie $V = W \oplus W^\perp = W^\perp \oplus W$ ve větě 3.74: záměnou role W a $W^\perp$ dostáváme $W^{\perp\perp} = W$ a $P_{W^\perp}\boldsymbol{x} = \boldsymbol{x}^\perp = \boldsymbol{x} - \boldsymbol{x}^\perp = I\boldsymbol{x} - P_W\boldsymbol{x} = (I - P_W)\boldsymbol{x}$, takže $I - P_W = P_{W^\perp}$ je skutečně operátorem ortogonální projekce. $\square$

D.46. DŮKAZ věty 3.76:

(1) $\boxed{\Rightarrow}$ $\boldsymbol{x} \in W \Rightarrow P_{W_1}\boldsymbol{x} = \boldsymbol{x}$, neboť $\boldsymbol{x} = \boldsymbol{x} + \boldsymbol{0}$, kde $\boldsymbol{0}$ je kolmý na

každý vektor (viz 3.65) a tedy zejména $\mathbf{0} \in W^\perp$ (tvrzení plyne též přímo z 3.52 a 3.53, protože P_W je dle 3.74 projekční operátor).
$\boxed{\Leftarrow}$ $P_{W_1}\boldsymbol{x} = \boldsymbol{x} \Rightarrow \boldsymbol{x} \in W_1$, neboť $P_{W_1}\boldsymbol{x} \in W_1$.

(2) $\boldsymbol{x} \in W_1^\perp \overset{3.75\&(1)}{\Leftrightarrow} (I - P_{W_1})\boldsymbol{x} = \boldsymbol{x} \Leftrightarrow \boldsymbol{x} - P_{W_1}\boldsymbol{x} = \boldsymbol{x} \Leftrightarrow P_{W_1}\boldsymbol{x} = \mathbf{0}$.
(3) Pro každé $\boldsymbol{x} \in V$ platí $\boldsymbol{x} = P_{W_1}\boldsymbol{x} + \boldsymbol{x}^\perp$, $\boldsymbol{x}^\perp \in W_1^\perp$ a tedy $P_{W_2}\boldsymbol{x} = P_{W_2}(P_{W_1}\boldsymbol{x}) + P_{W_2}\boldsymbol{x}^\perp$.
Odtud: $P_{W_2}\boldsymbol{x} = P_{W_2}(P_{W_1}\boldsymbol{x})\ \forall \boldsymbol{x} \in V \Leftrightarrow P_{W_2}\boldsymbol{x}^\perp = \mathbf{0}\ \forall \boldsymbol{x} \in V \overset{*}{\Leftrightarrow} P_{W_2}\boldsymbol{y} = \mathbf{0}\ \forall \boldsymbol{y} \in W_1^\perp \overset{(2)}{\Leftrightarrow} \boldsymbol{y} \in W_2^\perp\ \forall \boldsymbol{y} \in W_1^\perp \Leftrightarrow W_1^\perp \subseteq W_2^\perp \overset{3.71}{\Leftrightarrow} W_2 \subseteq W_1$ s uvážením identit $W_1 = W_1^{\perp\perp}, W_2 = W_2^{\perp\perp}$ plynoucích z 3.75.
Zdůvodněme ještě podrobněji implikaci $\overset{*}{\Rightarrow}$ (opačná implikace $\overset{*}{\Leftarrow}$ je zřejmá, neboť $\boldsymbol{x}^\perp \in W_1^\perp$): Libovolné $\boldsymbol{y} \in W_1^\perp$ lze uvážit v roli $\boldsymbol{x}$, neboť $W_1^\perp \subseteq V$. Jelikož $P_{W_1}\boldsymbol{y} \overset{(2)}{=} \mathbf{0}$, tak $\boldsymbol{y} = \boldsymbol{y}^\perp$ a $P_{W_2}\boldsymbol{y} = P_{W_2}\boldsymbol{y}^\perp = \mathbf{0}$. □

D.47. DŮKAZ věty 3.77:
a) Vlastnost nejlepší aproximace: Buď $\boldsymbol{x} \in V$ libovolně, ale pevně zvolený. Pak pro každé $\boldsymbol{y} \in W$ dostáváme: $\boldsymbol{x} - \boldsymbol{y} = \underbrace{\boldsymbol{x} - \widehat{\boldsymbol{x}}}_{=\boldsymbol{x}^\perp} + \underbrace{\widehat{\boldsymbol{x}} - \boldsymbol{y}}_{\in W}$
$\overset{S11}{\Rightarrow} \|\boldsymbol{x} - \boldsymbol{y}\|^2 = \|\boldsymbol{x} - \widehat{\boldsymbol{x}}\|^2 + \underbrace{\|\widehat{\boldsymbol{x}} - \boldsymbol{y}\|^2}_{\geq 0} \geq \|\boldsymbol{x} - \widehat{\boldsymbol{x}}\|^2$. Tedy $\|\boldsymbol{x} - \widehat{\boldsymbol{x}}\|$ je nejmenší prvek uspořádané množiny $\{\|\boldsymbol{x} - \boldsymbol{y}\| \mid \boldsymbol{y} \in W\}$ a tudíž její infimum dle 2.25.
b) $\widehat{\boldsymbol{x}}$ je jediný: Nechť $\widetilde{\boldsymbol{x}} \in W$ je prvek s vlastností $\|\boldsymbol{x} - \widetilde{\boldsymbol{x}}\| = \|\boldsymbol{x} - \widehat{\boldsymbol{x}}\| = \inf_{\boldsymbol{y} \in W}\|\boldsymbol{x} - \boldsymbol{y}\|$. Položíme-li $\boldsymbol{y} = \widetilde{\boldsymbol{x}}$ v důkazu a), pak $\|\boldsymbol{x} - \widetilde{\boldsymbol{x}}\|^2 = \|\boldsymbol{x} - \widehat{\boldsymbol{x}}\|^2 + \|\widehat{\boldsymbol{x}} - \widetilde{\boldsymbol{x}}\|^2 \Rightarrow 0 = \|\widehat{\boldsymbol{x}} - \widetilde{\boldsymbol{x}}\|^2 \overset{N3}{\Rightarrow} \widehat{\boldsymbol{x}} = \widetilde{\boldsymbol{x}}$.
c) Souřadnice prvku $\widehat{\boldsymbol{x}}$: Je-li $W = \mathcal{L}(E)$, kde E je ONB ve W, pak $\beta_i = \langle \widehat{\boldsymbol{x}}, \boldsymbol{e}_i \rangle = \langle \boldsymbol{x} - \boldsymbol{x}^\perp, \boldsymbol{e}_i \rangle = \langle \boldsymbol{x}, \boldsymbol{e}_i \rangle - \underbrace{\langle \boldsymbol{x}^\perp, \boldsymbol{e}_i \rangle}_{=0} = \langle \boldsymbol{x}, \boldsymbol{e}_i \rangle$ je dle 3.69 jediné souřadnicové vyjádření. □

D.48. DŮKAZ věty 3.78:
Indukcí vzhledem k n:
$n=1$: $\boldsymbol{e}_1 = \boldsymbol{v}_1 \overset{3.17(2)}{\neq} \boldsymbol{0}$ je báze ve $W = W_1 = \mathcal{L}(\boldsymbol{e}_1)$, která je triviálně ortogonální, neboť je jednoprvková.
Indukční krok pro $n > 1$: Podle indukčního předpokladu (I.P.) nechť tvrzení platí pro $n-1$. Zřejmě $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{n-1}$ je lineárně nezávislá (viz 3.17(1)) a tedy dle 3.19(3) tvoří bázi ve $W_{n-1} := \mathcal{L}(\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_{n-1}\})$. Dle I.P. je $W_{n-1} = \mathcal{L}(\{\boldsymbol{e}_1, \dots, \boldsymbol{e}_{n-1}\})$, kde $\boldsymbol{e}_1, \dots, \boldsymbol{e}_{n-1}$ je ortogonální báze, tj. zejména $\boldsymbol{e}_j \perp \boldsymbol{e}_k$ pro $j \neq k$ a $\boldsymbol{e}_j \neq \boldsymbol{0}$; $j, k \in \{1, \dots, n-1\}$. Ukážeme, že totéž platí i po doplnění této báze o prvek $\boldsymbol{e}_n$:

- ortogonalita: $\boldsymbol{e}_n = \boldsymbol{v}_n - P_{W_{n-1}} \boldsymbol{v}_n \overset{3.74}{\in} W_{n-1}^{\perp} \Rightarrow \boldsymbol{e}_n \perp \{\boldsymbol{e}_1, \dots, \boldsymbol{e}_{n-1}\}$ a tedy celkem máme $\boldsymbol{e}_j \perp \boldsymbol{e}_k$ pro každé $j, k \in \{1, \dots, n\}, j \neq k$.
- $\boldsymbol{e}_n \neq \boldsymbol{0}$ sporem: Kdyby $\boldsymbol{e}_n = \boldsymbol{0}$, pak $\boldsymbol{v}_n = P_{W_{n-1}} \boldsymbol{v}_n \in W_{n-1} = \mathcal{L}(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{n-1}) \overset{3.18}{\Rightarrow} \boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ jsou lineárně závislé, takže dle 3.19(3) nemohou tvořit bázi, spor s předpokladem věty.
- $\mathcal{L}(\{\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\}) \overset{?}{=} W_n$: Inkluze $\subseteq$ je zřejmá, neboť $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n \in W_n$.

$$\left.\begin{array}{l} \boldsymbol{v}_1, \dots, \boldsymbol{v}_{n-1} \in W_{n-1} = \mathcal{L}(\{\boldsymbol{e}_1, \dots, \boldsymbol{e}_{n-1}\}) \subseteq \mathcal{L}(\{\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\}) \\ \boldsymbol{v}_n = \boldsymbol{e}_n + \sum_{j=1}^{n-1} \frac{\langle \boldsymbol{v}_n, \boldsymbol{e}_j \rangle}{\|\boldsymbol{e}_j\|^2} \boldsymbol{e}_j \in \mathcal{L}(\{\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\}) \end{array}\right\} \overset{3.14(2)}{\Rightarrow}$$

$W_n = \mathcal{L}(\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_n\}) \subseteq \mathcal{L}(\{\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\})$.
Celkem tedy $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ je ortogonální báze ve W podle 3.68.
Výpočet projekce v k-tém kroku:
$P_{W_{k-1}} \boldsymbol{v}_k \overset{3.77}{=} \sum_{j=1}^{k-1} \langle \boldsymbol{v}_k, \frac{\boldsymbol{e}_j}{\|\boldsymbol{e}_j\|} \rangle \frac{\boldsymbol{e}_j}{\|\boldsymbol{e}_j\|} \overset{S6}{=} \sum_{j=1}^{k-1} \frac{1}{\|\boldsymbol{e}_j\|} \langle \boldsymbol{v}_k, \boldsymbol{e}_j \rangle \frac{\boldsymbol{e}_j}{\|\boldsymbol{e}_j\|}$, neboť $\{\frac{\boldsymbol{e}_j}{\|\boldsymbol{e}_j\|}\}_{j=1}^k$ je dle 3.66(b) ortonormální báze vzniklá normalizací ortogonální báze $\{\boldsymbol{e}_j\}_{j=1}^k$. □

D.49. DŮKAZ věty 3.79:
Tvrzení o existenci OB, resp. ONB plyne z toho, že dle 3.24(2) má každý vektorový prostor bázi, kterou lze dle 3.78 ortogonalizovat a případně dle 3.66(b) i normalizovat.

Tvrzení o doplnění plyne z toho, že každá ortogonální množina s nenulovými prvky je dle 3.68 lineárně nezávislá, takže ji lze dle 3.24(1) doplnit na bázi a tu pak ortogonalizovat užitím 3.78, kde zřejmě dostaneme $\boldsymbol{e}_j = \boldsymbol{v}_j$, pokud $\boldsymbol{v}_j$ jsou pro $j = 1, \ldots, k$ již ortogonální. Totiž suma ve vztahu pro $\boldsymbol{v}_k$ se vynuluje v důsledku $\boldsymbol{v}_k \perp W_{k-1}$, kdy $\langle \boldsymbol{v}_k, \boldsymbol{e}_j \rangle = 0$ pro $j = 1, \ldots, k-1$. $\square$

D.50. DŮKAZ věty 3.80:
Nechť $\dim W =: n < \infty$. Vzhledem k 3.73 stačí ukázat $V = W + W^{\perp}$. K tomu stačí ověřit $V \subseteq W + W^{\perp}$, neboť opačná inkluze platí vždy. Podle 3.79 existuje ve W nějaká ONB, označme ji $E =: \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$. Zvolme $\boldsymbol{x} \in V$ libovolně a položme $\boldsymbol{w} := \sum_{i=1}^{n} \langle \boldsymbol{x}, \boldsymbol{e}_i \rangle \boldsymbol{e}_i \in W$. Potom $\boldsymbol{x} - \boldsymbol{w} \perp E$, neboť $\langle \boldsymbol{x} - \sum_{i=1}^{n} \langle \boldsymbol{x}, \boldsymbol{e}_i \rangle \boldsymbol{e}_i, \boldsymbol{e}_j \rangle \overset{S1}{=} \langle \boldsymbol{x}, \boldsymbol{e}_j \rangle - \sum_{i=1}^{n} \langle \boldsymbol{x}, \boldsymbol{e}_i \rangle \langle \boldsymbol{e}_i, \boldsymbol{e}_j \rangle$ $= \langle \boldsymbol{x}, \boldsymbol{e}_j \rangle - \langle \boldsymbol{x}, \boldsymbol{e}_j \rangle = 0$ pro každé j vzhledem k ortonormalitě E, kdy $\langle \boldsymbol{e}_i \boldsymbol{e}_j \rangle = 0$ pro $i \neq j$ a $\langle \boldsymbol{e}_j \boldsymbol{e}_j \rangle = \|\boldsymbol{e}_j\|^2 = 1$. Podle 3.72 je $\boldsymbol{x} - \boldsymbol{w} \perp W$ a $\boldsymbol{x} = \underbrace{\boldsymbol{w}}_{\in W} + \underbrace{\boldsymbol{x} - \boldsymbol{w}}_{\in W^{\perp}} \overset{3.45(2)}{\Rightarrow} \boldsymbol{x} \in W + W^{\perp}$. $\square$

D.51. Důkaz věty 3.82:
a) <u>Jednoznačnost:</u> Nechť T^* a T' jsou dvě zobrazení s vlastností:
$\langle T\boldsymbol{x}, \boldsymbol{y} \rangle = \langle \boldsymbol{x}, T^*\boldsymbol{y} \rangle = \langle \boldsymbol{x}, T'\boldsymbol{y} \rangle \ \forall\, \boldsymbol{x} \in V_1$ a $\forall\, \boldsymbol{y} \in V_2 \overset{S5}{\Rightarrow}$
$0 = \langle \boldsymbol{x}, T^*\boldsymbol{y} - T'\boldsymbol{y} \rangle \ \forall\, \boldsymbol{x} \in V_1$ a $\forall\, \boldsymbol{y} \in V_2 \Rightarrow$ speciálně pro $\boldsymbol{x} = T^*\boldsymbol{y} - T'\boldsymbol{y}$ dostáváme $0 = \langle T^*\boldsymbol{y} - T'\boldsymbol{y}, T^*\boldsymbol{y} - T'\boldsymbol{y} \rangle \ \forall\, \boldsymbol{y} \in V_2 \overset{S4}{\Rightarrow} T^*\boldsymbol{y} - T'\boldsymbol{y} = \boldsymbol{0}$ $\forall\, \boldsymbol{y} \in V_2 \Rightarrow T^*\boldsymbol{y} = T'\boldsymbol{y} \ \forall\, \boldsymbol{y} \in V_2 \Rightarrow T^* = T'$.
b) <u>Linearita T^*:</u> Pro libovolná $\boldsymbol{x} \in V_1$, $\boldsymbol{y}, \boldsymbol{y}_1, \boldsymbol{y}_2 \in V_2$ a $\alpha \in \mathbb{F}$ je třeba ověřit vlastnosti (1) a (2) z věty 3.27:
(1) $\langle \boldsymbol{x}, T^*(\boldsymbol{y}_1 + \boldsymbol{y}_2) \rangle = \langle T\boldsymbol{x}, \boldsymbol{y}_1 + \boldsymbol{y}_2 \rangle \overset{S5}{=} \langle T\boldsymbol{x}, \boldsymbol{y}_1 \rangle + \langle T\boldsymbol{x}, \boldsymbol{y}_2 \rangle = \langle \boldsymbol{x}, T^*\boldsymbol{y}_1 \rangle +$ $\langle \boldsymbol{x}, T^*\boldsymbol{y}_2 \rangle \overset{S5}{=} \langle \boldsymbol{x}, T^*\boldsymbol{y}_1 + T^*\boldsymbol{y}_2 \rangle \overset{a)}{\Rightarrow} T^*(\boldsymbol{y}_1 + \boldsymbol{y}_2) = T^*\boldsymbol{y}_1 + T^*\boldsymbol{y}_2$.
(2) $\langle \boldsymbol{x}, T^*(\alpha\boldsymbol{y}) \rangle = \langle T\boldsymbol{x}, \alpha\boldsymbol{y} \rangle \overset{S6}{=} \overline{\alpha} \langle T\boldsymbol{x}, \boldsymbol{y} \rangle = \overline{\alpha} \langle \boldsymbol{x}, T^*\boldsymbol{y} \rangle \overset{S6}{=} \langle \boldsymbol{x}, \alpha T^*\boldsymbol{y} \rangle$ $\overset{a)}{\Rightarrow} T^*(\alpha\boldsymbol{y}) = \alpha T^*\boldsymbol{y}$. $\square$

D.52. DŮKAZ věty 3.85:
Pro libovolně zvolené prvky $\boldsymbol{x} \in V_1$, $\boldsymbol{y} \in V_2$, $\boldsymbol{z} \in V_3$ ověříme (1)–(4).

Využijeme přitom jednoznačnosti adjungovaného operátoru garantované větou 3.82:
(1) $\langle T^*\boldsymbol{y}, \boldsymbol{x}\rangle \overset{S3}{=} \overline{\langle \boldsymbol{x}, T^*\boldsymbol{y}\rangle} = \overline{\langle T\boldsymbol{x}, \boldsymbol{y}\rangle} \overset{S3}{=} \langle \boldsymbol{y}, T\boldsymbol{x}\rangle \overset{3.82}{\Rightarrow} T = T^{**}$.
(2) $\langle (UT)\boldsymbol{x}, \boldsymbol{z}\rangle = \langle U(T\boldsymbol{x}), \boldsymbol{z}\rangle = \langle T\boldsymbol{x}, U^*\boldsymbol{z}\rangle = \langle \boldsymbol{x}, T^*(U^*\boldsymbol{z})\rangle = \langle \boldsymbol{x}, (T^*U^*)\boldsymbol{z})\rangle$
$\overset{3.82}{\Rightarrow} (UT)^* = T^*U^*$.
(3) $\langle I\boldsymbol{x}, \boldsymbol{y}\rangle = \langle \boldsymbol{x}, \boldsymbol{y}\rangle = \langle \boldsymbol{x}, I\boldsymbol{y}\rangle \overset{3.82}{\Rightarrow} I^* = I$.
(4) $(T^*T)^* \overset{(2)}{=} T^*T^{**} \overset{(1)}{=} T^*T$ a podobně $(TT^*)^* \overset{(2)}{=} T^{**}T^* \overset{(1)}{=} TT^*$
$\Rightarrow TT^*$ i T^*T jsou samoadjungované operátory.
Dále s uvážením 3.84 platí:
$\langle T^*T\boldsymbol{x}, \boldsymbol{x}\rangle = \langle T\boldsymbol{x}, T^{**}\boldsymbol{x}\rangle \overset{(1)}{=} \langle T\boldsymbol{x}, T\boldsymbol{x}\rangle \overset{S4}{\geq} 0 \Rightarrow T^*T$ je pozitivní.
$\langle TT^*\boldsymbol{y}, \boldsymbol{y}\rangle = \langle T^*\boldsymbol{y}, T^*\boldsymbol{y}\rangle \overset{S4}{\geq} 0 \Rightarrow TT^*$ je pozitivní.
□

D.53. Důkaz věty 3.86:
$\boxed{(1) \Rightarrow (2)}$ $P = P_W \overset{3.74}{\Rightarrow} \ \forall \boldsymbol{x} \in V : \boldsymbol{x} = P_W\boldsymbol{x} + \boldsymbol{x}^\perp$, kde $\boldsymbol{x}^\perp \in W^\perp$
$\Rightarrow \boldsymbol{x} - P_W\boldsymbol{x} \perp W$.
$\boxed{(2) \Rightarrow (1)}$ $W + W^\perp \subseteq V$ platí triviálně. Naopak $V \subseteq W + W^\perp$ rovněž platí, neboť pro každé $\boldsymbol{x} \in V$ je $\boldsymbol{x} = \underbrace{P\boldsymbol{x}}_{\in W} + \underbrace{\boldsymbol{x} - P\boldsymbol{x}}_{\in W^\perp}$. Tedy celkem $V = W + W^\perp = W \oplus W^\perp$, přičemž z jednoznačnosti tohoto rozkladu (ortogonální součet je totiž přímým součtem dle 3.73) dostáváme $P_W\boldsymbol{x} = P\boldsymbol{x} \ \forall \boldsymbol{x} \in V \Rightarrow P = P_W$ je operátorem ortogonální projekce na W.
$\boxed{(1) \Rightarrow (3)}$ Je-li P operátorem ortogonální projekce (tj. $P = P_W$), pak je dle 3.74 speciálním případem projekčního operátoru a tudíž lineární a splňuje $P^2 = P$ (viz 3.52, 3.53). Vlastnost $P^2 = P$ můžeme ověřit i přímo: $\boldsymbol{u} := P\boldsymbol{x} \in W$; $P\boldsymbol{u} \in W \Rightarrow \boldsymbol{u} - P\boldsymbol{u} \in W \cap W^\perp = \{\boldsymbol{0}\}$
$\Rightarrow P\boldsymbol{x} = \boldsymbol{u} = P\boldsymbol{u} = P(P\boldsymbol{x}) = P^2\boldsymbol{x} \ \forall \boldsymbol{x} \in V$.
Zbývá ověřit samoadjungovanost $P = P^*$. Zvolme $\boldsymbol{x}, \boldsymbol{y} \in V$ libovolně.

Pak $\langle P\boldsymbol{x}, \boldsymbol{y}\rangle = \langle \widehat{\boldsymbol{x}}, \widehat{\boldsymbol{y}} + \boldsymbol{y}^{\perp}\rangle \overset{S5}{=} \langle \widehat{\boldsymbol{x}}, \widehat{\boldsymbol{y}}\rangle + \underbrace{\langle \widehat{\boldsymbol{x}}, \boldsymbol{y}^{\perp}\rangle}_{=0} = \langle \widehat{\boldsymbol{x}}, \widehat{\boldsymbol{y}}\rangle + \underbrace{\langle \boldsymbol{x}^{\perp}, \widehat{\boldsymbol{y}}\rangle}_{=0} \overset{S1}{=}$
$\langle \widehat{\boldsymbol{x}} + \boldsymbol{x}^{\perp}, \widehat{\boldsymbol{y}}\rangle = \langle \boldsymbol{x}, P\boldsymbol{y}\rangle$.

$\boxed{(3) \Rightarrow (2)}$ Položme $M := \{\boldsymbol{x} \in V \,|\, P\boldsymbol{x} = \boldsymbol{x}\}$. Zřejmě $M \subseteq W$. Platí i opačná inkluze. Totiž pro každé $\boldsymbol{x} \in V$ je $P\boldsymbol{x} \in M$, neboť $P\boldsymbol{x} = P^2\boldsymbol{x} = P(P\boldsymbol{x}) \Rightarrow W = \mathcal{R}(P) \subseteq M$. Celkem tedy $M = W$. Pak pro každé $\boldsymbol{u} \in M = W$ a $\boldsymbol{x} \in V$ dostáváme: $\langle \boldsymbol{x} - P\boldsymbol{x}, \boldsymbol{u}\rangle \overset{S1,S2}{=}$
$\langle \boldsymbol{x}, \boldsymbol{u}\rangle - \langle P\boldsymbol{x}, \boldsymbol{u}\rangle = \langle \boldsymbol{x}, \boldsymbol{u}\rangle - \langle \boldsymbol{x}, P^*\boldsymbol{u}\rangle = \langle \boldsymbol{x}, \boldsymbol{u}\rangle - \langle \boldsymbol{x}, P\boldsymbol{u}\rangle =$
$\langle \boldsymbol{x}, \boldsymbol{u}\rangle - \langle \boldsymbol{x}, \boldsymbol{u}\rangle = 0$. Tedy $\boldsymbol{x} - P\boldsymbol{x} \perp W$ pro každé $\boldsymbol{x} \in V$. □

D.54. DŮKAZ věty 3.87:
3.86(3) $\Rightarrow P = P\,P = P^*P \overset{3.85(4)}{\Rightarrow} P$ je pozitivní. □

D.55. Důkaz věty 3.88:
(1) $\boldsymbol{x} \in \mathcal{N}(T) \;\Leftrightarrow\; T\boldsymbol{x} = \mathbf{0} \;\overset{*}{\Leftrightarrow}\; \langle T\boldsymbol{x}, \boldsymbol{y}\rangle = 0 \;\forall\, \boldsymbol{y} \in V_2 \;\Leftrightarrow\; \langle \boldsymbol{x}, T^*\boldsymbol{y}\rangle = 0$ $\forall\, \boldsymbol{y} \in V_2 \;\Leftrightarrow\; \boldsymbol{x} \in \mathcal{R}(T^*)^{\perp}$.
Zdůvodněme ještě podrobněji implikaci $\overset{*}{\Leftarrow}$ (opačná implikace $\overset{*}{\Rightarrow}$ je důsledkem S7): položíme-li $\boldsymbol{y} = T\boldsymbol{x}$, pak $\langle T\boldsymbol{x}, T\boldsymbol{x}\rangle = 0 \overset{S4}{\Rightarrow} T\boldsymbol{x} = \mathbf{0}$.
Záměnou role T a T^* dostáváme $\mathcal{N}(T^*) = \mathcal{R}(T^{**})^{\perp} \overset{3.85(1)}{=} \mathcal{R}(T)^{\perp}$.
(2) je speciálním případem (1) při $T = T^*$.
(3) • $\underline{\mathcal{N}(T) \overset{?}{\subseteq} \mathcal{N}(T^*T)}$: $\boldsymbol{x} \in \mathcal{N}(T) \Rightarrow T\boldsymbol{x} = \mathbf{0} \Rightarrow T^*T\boldsymbol{x} = T^*\mathbf{0} = \mathbf{0}$ $\Rightarrow \boldsymbol{x} \in \mathcal{N}(T^*T)$.
• $\underline{\mathcal{N}(T) \overset{?}{\supseteq} \mathcal{N}(T^*T)}$: $\boldsymbol{x} \in \mathcal{N}(T^*T) \Rightarrow T^*T\boldsymbol{x} = \mathbf{0} \overset{S7}{\Rightarrow} 0 = \langle \boldsymbol{x}, T^*T\boldsymbol{x}\rangle \overset{3.82}{=}$ $\langle T\boldsymbol{x}, T\boldsymbol{x}\rangle \overset{S4}{\Rightarrow} T\boldsymbol{x} = \mathbf{0} \Rightarrow \boldsymbol{x} \in \mathcal{N}(T)$.
• $\underline{\mathcal{N}(T^*) \overset{?}{=} \mathcal{N}(TT^*)}$ plyne z již dokázaného záměnou role T a T^*: $\mathcal{N}(TT^*) \overset{3.85(1)}{=} \mathcal{N}(T^{**}T^*) = \mathcal{N}(T^*)$.
(4) T surjektivní $\Rightarrow \mathcal{R}(T) = V_2 \Rightarrow \mathcal{N}(T^*) \overset{(1)}{=} \mathcal{R}(T)^{\perp} = V_2^{\perp} = \{\mathbf{0}\}$, neboť jediný prvek ve V_2 kolmý na V_2 a tedy i kolmý sám na sebe je dle 3.65 právě jen nulový prvek. Pro T^* se analogické tvrzení dokáže opět záměnou role T a T^*.

(5) Nechť například $\dim \mathcal{R}(T) < \infty$.

(i) $V_2 \overset{3.80}{=} \mathcal{R}(T) \oplus \mathcal{R}(T)^\perp \overset{(1)}{=} \mathcal{R}(T) \oplus \mathcal{N}(T^*)$.

(ii) $V_2 \overset{(i)}{=} \mathcal{N}(T^*) \oplus \mathcal{R}(T) \overset{3.74}{\Rightarrow} \mathcal{R}(T) = \mathcal{N}(T^*)^\perp$.

(iii) $\underline{\text{a) } \mathcal{R}(TT^*) \overset{?}{=} \mathcal{R}(T)\text{:}}$ Inkluze $\mathcal{R}(TT^*) \subseteq \mathcal{R}(T)$ je zřejmá, neboť každý prvek $\boldsymbol{y} \in \mathcal{R}(TT^*)$ je tvaru $\boldsymbol{y} = TT^*\boldsymbol{y}'$, kde $T^*\boldsymbol{y}' \in V_1$ a tedy $\boldsymbol{y} \in \mathcal{R}(T)$. Pak $\dim \mathcal{R}(TT^*) \leq \dim \mathcal{R}(T)$ dle 3.24(3) a (ii) lze tak aplikovat i na operátor $TT^* : V_2 \to V_2$: $\mathcal{R}(TT^*) \overset{(ii)}{=} \mathcal{N}((TT^*)^*)^\perp \overset{3.85(4)}{=} \mathcal{N}(TT^*)^\perp \overset{(3)}{=} \mathcal{N}(T^*)^\perp \overset{(ii)}{=} \mathcal{R}(T)$.

$\underline{\text{b) } \mathcal{R}(T^*T) \overset{?}{=} \mathcal{R}(T^*)\text{:}}$ Inkluze $\mathcal{R}(T^*T) \subseteq \mathcal{R}(T^*)$ platí analogicky jako v případě a). K důkazu opačné inkluze je však třeba užít jiný postup, neboť není garantována konečnost dimenze prostoru $\mathcal{R}(T^*)$: Libovolný prvek $\boldsymbol{x} \in \mathcal{R}(T^*)$ je tvaru $\boldsymbol{x} = T^*\boldsymbol{y}$, kde $V_2 \ni \boldsymbol{y} \overset{(i)}{=} \widehat{\boldsymbol{y}} + \boldsymbol{y}^\perp$, $\widehat{\boldsymbol{y}} \in \mathcal{R}(T)$, $\boldsymbol{y}^\perp \in \mathcal{N}(T^*)$. Pak ovšem $\boldsymbol{x} = T^*(\widehat{\boldsymbol{y}} + \boldsymbol{y}^\perp) = T^*\widehat{\boldsymbol{y}} + \underbrace{T^*\boldsymbol{y}^\perp}_{=\boldsymbol{0}} = T^*\widehat{\boldsymbol{y}} \in \mathcal{R}(T)$ a tedy existuje $\boldsymbol{x}' \in V_1$: $\widehat{\boldsymbol{y}} = T\boldsymbol{x}'$ a tudíž $\boldsymbol{x} = T^*T\boldsymbol{x}'$, takže $\boldsymbol{x} \in \mathcal{R}(T^*T)$.

(iv) $\mathcal{R}(T^*T) \overset{(iii)}{=} \mathcal{R}(T^*) \Rightarrow T^*|_{\mathcal{R}(T)}$ je surjekce na $\mathcal{R}(T^*)$ a tedy $\mathcal{R}(T^*|_{\mathcal{R}(T)}) = \mathcal{R}(T^*)$.

$\mathcal{N}(T^*|_{\mathcal{R}(T)}) = \{\boldsymbol{y} \in \mathcal{R}(T) \,|\, T^*\boldsymbol{y} = \boldsymbol{0}\} = \mathcal{R}(T) \cap \mathcal{N}(T^*) \overset{(ii)}{=} \mathcal{N}(T^*)^\perp \cap \mathcal{N}(T^*) = \{\boldsymbol{0}\}$, neboť dle 3.65 jedině nulový vektor může být kolmý sám na sebe. Celkem $T^*|_{\mathcal{R}(T)}$ je tedy podle 3.30(2) izomorfizmem. Podle 3.33 platí $\dim \mathcal{R}(T) = \dim \mathcal{R}(T^*) =: n < \infty$.

Při důkazu (iv) jsme ukázali, že také $\dim \mathcal{R}(T^*) < \infty$. Vzhledem k rovnosti $T^{**} \overset{3.85(1)}{=} T$ můžeme všude v (5) provést záměny $T \rightsquigarrow T^*$, $T^* \rightsquigarrow T$, $V_1 \rightsquigarrow V_2$ a $V_2 \rightsquigarrow V_1$, což dá duální tvrzení dosud nedokázaná v (i),(ii) a (iv): $V_2 = \mathcal{R}(T) \oplus \mathcal{N}(T^*) \rightsquigarrow V_1 = \mathcal{R}(T^*) \oplus \mathcal{N}(T)$, $\mathcal{N}(T^*)^\perp = \mathcal{R}(T) \rightsquigarrow \mathcal{N}(T)^\perp = \mathcal{R}(T^*)$ a

$T^*|_{\mathcal{R}(T)}$ je izomorfizmus $\rightsquigarrow T|_{\mathcal{R}(T^*)}$ je izomorfizmus .
Z týchž důvodů je možno (5) analogicky dokazovat s výchozím předpokladem $\dim \mathcal{R}(T^*) < \infty$ namísto zde užitého $\dim \mathcal{R}(T) < \infty$.

(v) je důsledkem (i) a vět 3.73 a 3.49.

(vi) T izomorfizmus $\overset{3.30(2)}{\Rightarrow} \mathcal{N}(T) = \{\mathbf{0}\} \overset{(i)}{\Rightarrow} V_1 = \mathcal{R}(T^*) \Rightarrow T^*$ je surjektivní. Protože T je také surjektivní, tak podle (4) je T^* současně izomorfním vnořením. Celkem tedy T^* je izomorfizmus.
Buďte $\boldsymbol{x} \in V_1$ a $\boldsymbol{y} \in V_2$ libovolně zvolené prvky. Jelikož T^* je izomorfizmus a tudíž surjekce, tak $\boldsymbol{x} = T^*\boldsymbol{y}'$ pro vhodné $\boldsymbol{y}' \in V_2$. Pak $\langle T^{-1}\boldsymbol{y}, \boldsymbol{x}\rangle = \langle T^{-1}\boldsymbol{y}, T^*\boldsymbol{y}'\rangle = \langle TT^{-1}\boldsymbol{y}, \boldsymbol{y}'\rangle = \langle \boldsymbol{y}, \boldsymbol{y}'\rangle = \langle \boldsymbol{y}, (T^*)^{-1}\boldsymbol{x}\rangle$ a tedy $(T^{-1})^* = (T^*)^{-1}$ vzhledem k jednoznačnosti dle 3.82.

□

D.56. Důkaz věty 3.90:

$\boxed{(1) \Rightarrow (3)}$ T unitární $\Rightarrow$ pro nějakou ONB E ve V_1 je $T(E)$ rovněž ONB ve V_2 téže mohutnosti, zejména tedy je zobrazení $T : E_1 \to E_2$ bijekcí. Zvolme $\boldsymbol{x}, \boldsymbol{y} \in V_1$ libovolně. Pak podle 3.69 existuje konečně mnoho $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n \in E$, $\boldsymbol{e}_i \neq \boldsymbol{e}_j$ pro $i \neq j$ tak, že $\boldsymbol{x} = \sum_{i=1}^n \xi_i \boldsymbol{e}_i$ a $\boldsymbol{y} = \sum_{j=1}^n \eta_j \boldsymbol{e}_j$. Pak $T\boldsymbol{x} = \sum_{i=1}^n \xi_i T\boldsymbol{e}_i$ a $T\boldsymbol{y} = \sum_{j=1}^n \eta_j T\boldsymbol{e}_j$, kde $T\boldsymbol{e}_i \neq T\boldsymbol{e}_j$ pro $i \neq j$. Oba vektory i jejich obrazy mají tedy stejné souřadnice v ONB E i v ONB $T(E)$, takže dle 3.70 platí:
$\langle T\boldsymbol{x}, T\boldsymbol{y}\rangle = \sum_{i=1}^n \sum_{j=1}^n \xi \overline{\eta}_j = \langle \boldsymbol{x}, \boldsymbol{y}\rangle$.
T je také surjektivní, neboť je dle 3.89 izomorfizmem.

$\boxed{(3) \Rightarrow (2)}$

• <u>T je izomorfizmus:</u> $\boldsymbol{x} \in \mathcal{N}(T) \Rightarrow T\boldsymbol{x} = \mathbf{0} \Rightarrow 0 \overset{S4}{=} \langle T\boldsymbol{x}, T\boldsymbol{x}\rangle \overset{(3)}{=} \langle \boldsymbol{x}, \boldsymbol{x}\rangle \overset{S4}{\Rightarrow} \boldsymbol{x} = \mathbf{0}$, takže $\mathcal{N}(T) = \{\mathbf{0}\}$. Současně také platí $\mathcal{R}(T) = V_2$, neboť T je surjekce. Celkem je tedy T izomorfizmus podle 3.30(2).
• <u>T zachovává ortonormální báze:</u> Je-li E libovolná ONB ve V_1, pak $T(E)$ je podle 3.30(4) bází ve V_2 téže mohutnosti. Zbývá ověřit její ortonormalitu:

a) Pro každý prvek $T\boldsymbol{e} \in T(E)$ je
$\|T\boldsymbol{e}\| \overset{S9}{=} \sqrt{\langle T\boldsymbol{e}, T\boldsymbol{e}\rangle} \overset{(3)}{=} \sqrt{\langle \boldsymbol{e}, \boldsymbol{e}\rangle} \overset{S9}{=} \|\boldsymbol{e}\| = 1$.
b) Pro libovolné dva prvky $T\boldsymbol{e}_1, T\boldsymbol{e}_2 \in T(E)$, $T\boldsymbol{e}_1 \neq T\boldsymbol{e}_2$ jistě platí také $\boldsymbol{e}_1 \neq \boldsymbol{e}_2$, $\boldsymbol{e}_1 \perp \boldsymbol{e}_2$, takže $\langle T\boldsymbol{e}_1, T\boldsymbol{e}_2\rangle \overset{(3)}{=} \langle \boldsymbol{e}_1, \boldsymbol{e}_2\rangle = 0 \Rightarrow T\boldsymbol{e}_1 \perp T\boldsymbol{e}_2$.
$\boxed{(2) \Rightarrow (1)}$ Podle předpokladu věty existuje ve V_1 alespoň jedna ONB, která se při platnosti (2) zobrazí na ONB ve V_2 téže mohutnosti, takže T je podle definice 3.89 unitární.
$\boxed{(3) \Rightarrow (4)}$ $\|T\boldsymbol{x}\| \overset{S9}{=} \sqrt{\langle T\boldsymbol{x}, T\boldsymbol{x}\rangle} \overset{(3)}{=} \sqrt{\langle \boldsymbol{x}, \boldsymbol{x}\rangle} \overset{S9}{=} \|\boldsymbol{x}\| \ \forall \boldsymbol{x} \in V_1$, kde T je surjektivní.
$\boxed{(4) \Rightarrow (3)}$ Pro libovolné $\boldsymbol{x}, \boldsymbol{y} \in V_1$ lze výpočtem opírajícím se o (S9) a bilinearitu 3.1 skalárního součinu ověřit (cvičení) platnost tzv. polarizační identity (viz též důkaz rovnoběžníkového zákona D.36) [27]:

$$\langle \boldsymbol{x}, \boldsymbol{y}\rangle = \frac{1}{4}\{\|\boldsymbol{x}+\boldsymbol{y}\|^2 - \|\boldsymbol{x}-\boldsymbol{y}\|^2 + i(\|\boldsymbol{x}+i\boldsymbol{y}\|^2 - \|\boldsymbol{x}-i\boldsymbol{y}\|^2)\} \text{ ve } V_1$$

a

$$\begin{aligned}\langle T\boldsymbol{x}, T\boldsymbol{y}\rangle = \frac{1}{4}\{&\|T\boldsymbol{x}+T\boldsymbol{y}\|^2 - \|T\boldsymbol{x}-T\boldsymbol{y}\|^2 + \\ &+ i(\|T\boldsymbol{x}+iT\boldsymbol{y}\|^2 - \|T\boldsymbol{x}-iT\boldsymbol{y}\|^2)\} \text{ ve } V_2,\end{aligned}$$

kde $\|T\boldsymbol{x} \pm T\boldsymbol{y}\| = \|T(\boldsymbol{x} \pm \boldsymbol{y})\| \overset{(4)}{=} \|\boldsymbol{x} \pm \boldsymbol{y}\|$ a podobně $\|T\boldsymbol{x} \pm iT\boldsymbol{y}\| = \|T(\boldsymbol{x} \pm i\boldsymbol{y})\| \overset{(4)}{=} \|\boldsymbol{x} \pm i\boldsymbol{y}\|$ implikuje $\langle T\boldsymbol{x}, T\boldsymbol{y}\rangle = \langle \boldsymbol{x}, \boldsymbol{y}\rangle$.
$\boxed{(3) \Rightarrow (5)}$ Již byla ukázána ekvivalence (3) $\Leftrightarrow$ (1), takže T je unitární a zejména izomorfizmus dle 3.89. Proto T^{-1} existuje a pro každé $\boldsymbol{x} \in V_1$ a $\boldsymbol{y} \in V_2$ můžeme psát:
$\langle \boldsymbol{x}, T^{-1}\boldsymbol{y}\rangle \overset{(3)}{=} \langle T\boldsymbol{x}, TT^{-1}\boldsymbol{y}\rangle = \langle T\boldsymbol{x}, \boldsymbol{y}\rangle \overset{3.82}{\Rightarrow} T^* = T^{-1}$.
$\boxed{(5) \Rightarrow (6)}$ $T^* = T^{-1} \Rightarrow T^*T = T^{-1}T = I$ a $TT^* = TT^{-1} = I$.

---

[27] člen v kulaté závorce se dá upravit na tvar $2i(\langle \boldsymbol{y}, \boldsymbol{x}\rangle - \langle \boldsymbol{x}, \boldsymbol{y}\rangle)$, takže v případě $\mathbb{F} = \mathbb{R}$ se vynuluje v důsledku symetrie (S3').

$\boxed{(6) \Rightarrow (3)}$ $TT^* = I \Rightarrow T$ je surjekce a současně pro každé $\boldsymbol{x}, \boldsymbol{y} \in V_1$ platí $\langle T\boldsymbol{x}, T\boldsymbol{y}\rangle \overset{3.82}{=} \langle \boldsymbol{x}, T^*T\boldsymbol{y}\rangle = \langle \boldsymbol{x}, I\boldsymbol{y}\rangle = \langle \boldsymbol{x}, \boldsymbol{y}\rangle$.

Pokud T je unitární, tak T^{-1} rovněž: totiž pro každé $\boldsymbol{x}, \boldsymbol{y} \in V_2$ je $\langle T^{-1}\boldsymbol{x}, T^{-1}\boldsymbol{y}\rangle \overset{(3)}{=} \langle TT^{-1}\boldsymbol{x}, TT^{-1}\boldsymbol{y}\rangle = \langle \boldsymbol{x}, \boldsymbol{y}\rangle$, přičemž samozřejmě T^{-1} je izomorfizmus a tedy zejména surjektivní. Pro T^{-1} tak platí (3) a je proto unitární. $\square$

D.57. Důkaz důsledku 3.92:
$\dim V < \infty \overset{3.79}{\Rightarrow}$ ve V existuje ONB. Pak $[\cdot]_E : V \to \mathbb{F}^n$ je izomorfizmus dle 3.32 (tedy i surjekce), který je dokonce unitární na základě 3.90(3), neboť pro ONB $E =: \{\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\}$ a každé $\boldsymbol{x}, \boldsymbol{y} \in V$ dostáváme: $\langle \boldsymbol{x}, \boldsymbol{y}\rangle \overset{3.70}{=} \sum_{i=1}^n \xi_i \overline{\eta}_i \overset{3.64}{=} \langle \boldsymbol{\xi}, \boldsymbol{\eta}\rangle \overset{3.69}{=} \langle [\boldsymbol{x}]_E, [\boldsymbol{y}]_E\rangle$, kde $\xi_i = \langle \boldsymbol{x}, \boldsymbol{e}_i\rangle$ a $\eta_i = \langle \boldsymbol{y}, \boldsymbol{e}_i\rangle$. $\square$

D.58. Důkaz důsledku 3.93:
Protože v konečně rozměrných prostorech lze dle 3.79 vždy vybrat ortonormální báze, tak izomorfizmy, resp. izomorfní vnoření z důkazu D.30 důsledku 3.33 budou podle 3.92 unitární, jestliže navíc uvážíme triviální fakt, že skládáním unitárních izomorfizmů, resp. izomorfních vnoření dostáváme opět unitární izomorfizmus, resp. izomorfní vnoření. Totiž složení dvou lineárních zobrazení majících např. vlastnost 3.90(2), resp. 3.91(2') bude jistě zase lineární zobrazení s touž vlastností. $\square$