Petr Olšák

Výcuc

z textu Lineární algebra

určeno pro promítání na přednášce „Úvod do algebry“

http://www.olsak.net/linal.html
ftp://math.feld.cvut.cz/pub/olsak/linal/
http://math.feld.cvut.cz/skripta/ua/

Upozornění 1. Nedoporučuji tento text přímo tisknout. K tisku je vhodné použít text Lineární algebra a nikoli jeho výcuc. Nebo si můžete pořídit skripta Úvod do algebry, zejména lineární. Pokud přesto chcete tisknout výcuc, doporučuji použít následující verzi, kde jsou jednotlivé obrazovky uspořádány po čtyřech na stránce, tj. redukujete spotřebu kancelářských technologií na čtvrtinu.

Upozornění 2. Tento výcuc není určen k samostatnému studiu. Je pouze podporou přednášky. Jenom *absolutní mimoň* je schopen pročítat zde uvedené věty a definice bez ilustrací, bez vysvětlení významu vět, bez jejich použití v důkazech dalších vět a bez podpůrných příkladů. Tyto definice a věty jsou sice jádrem výuky předmětu Úvod do algebry, ale na přednáškách a cvičeních se budeme snažit, aby bylo toto jádro co nejpřístupnější. Proto na nich zazní množství ilustračních příkladů, komentářů a vysvětlení, které ovšem nejsou jádrem výuky tohoto předmětu, ale pomohou vám to jádro lépe pochopit.

Doporučení 1. Jak jste si asi všimli, zelený text je aktivní a můžete na něj kliknout k dosažení dalších informací. Aby byly všechny odkazy funkční, je potřeba mít kromě tohoto výcucu ve stejném adresáři i plný text Lineární algebra ve formátu PDF. Čísla po stranách definic a vět se shodují se stejnými čísly v plném textu a pokud na ně kliknete, objeví se příslušná pasáž plného textu (tedy například věta včetně důkazu).

Doporučení 2. Pokud si vytisknete tento výcuc (předpokládám, že v úsporné variantě), pak si například můžete na svůj výtisk vpisovat vysvětlující komentáře a důkazy vět, které uslyšíte na přednášce. Nemusíte se tam pak zdržovat přepisováním definic a vět, ale můžete se lépe soustředit na jejich pochopení.

Definice. *Polynom* je reálná funkce reálné proměnné (nebo komplexní funkce komplexní proměnné), která je dána vzorcem

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

kde $a_0, a_1, \ldots, a_n \in \mathbf{R}$ (nebo $\in \mathbf{C}$) jsou *koeficienty polynomu* a x je proměnná.
Polynom značíme malými písmeny p, q, p_1, p_2 atd. Připíšeme-li závorku za toto písmeno, např. $p(x)$, máme na mysli hodnotu polynomu v bodě x. Toto je obvyklé značení, jaké se používá pro libovolné funkce (nejen pro polynomy).
Stupeň polynomu je nejvyšší k takové, že koeficient $a_k \neq 0$. Jsou-li všechny koeficienty nulové, klademe stupeň roven -1. Takovému polynomu říkáme *nulový polynom*.

Věta. Polynom je jednoznačně určen svými koeficienty (ignorujeme nulové koeficienty s indexem větším než stupeň).
To znamená, že dva různé polynomy (ve smyslu různé funkce) mají odlišné koeficienty a obráceně polynomy zadané různými koeficienty jsou různé funkce.
Nulový polynom má všechny koeficienty nulové.

Věta. Součet a rozdíl polynomů je polynom. Násobek polynomu konstantou je polynom. Součin polynomů je polynom. Podíl polynomů nemusí být polynom.
Poznámka. Odvoďte si vzorce pro koeficienty polynomu, který je součtem, rozdílem a součinem polynomů se zadanými koeficienty. Odvoďte také vzorce pro stupeň součtu, rozdílu a součinu polynomů.

Věta. Polynomy p a q je možno „dělit se zbytkem".
Pro polynomy p, q (q nenulový) existují polynomy r a z s vlastnostmi:
(A) $p/q = r + z/q$, (B) stupeň z je menší než stupeň q.
Polynomu r v tomto kontextu říkáme *částečný podíl* a polynomu z říkáme *zbytek*.

Definice. *Kořen* polynomu p je takové číslo α (reálné nebo komplexní), pro které je $p(\alpha) = 0$.

Věta. Číslo α je kořenem polynomu p právě tehdy, když existuje polynom r takový, že $p(x) = (x - \alpha)\,r(x)$ pro všechna $x \in \mathbf{R}$ (nebo $x \in \mathbf{C}$).
Je-li α kořenem polynomu p, pak polynomu $(x-\alpha)$ říkáme *kořenový činitel* polynomu p.

Věta. (Základní věta algebry). Každý polynom stupně aspoň prvního má aspoň jeden komplexní kořen.

Důsledek věty. Každý polynom p stupně $n \geq 1$ lze rozepsat na součin kořenových činitelů:

$$p(x) = a\,(x - \alpha_1)\,(x - \alpha_2) \cdots (x - \alpha_n)$$

kde a je konstanta a $\alpha_i \in \mathbf{C}$ jsou všechny kořeny polynomu p.

V tomto zápise se stejné hodnoty kořenů mohou vyskytovat opakovaně. *Násobnost kořenu* je počet výskytů hodnoty tohoto kořenu v součinu kořenových činitelů.

Věta. Pro obecný polynom stupně pátého nebo vyššího nelze najít vzorec na výpočet kořenů polynomu z jeho koeficientů takový, který by se opíral o konečné množství operací sčítání, odečítání, násobení, dělení a odmocňování.

Poznámka 1. Tato věta není v rozporu se základní větou algebry. Kořeny vždy existují, ale často je neumíme najít.

Poznámka 2. Pokud se v tomto kurzu setkáte s příklady, které mají ilustrovat rozklad polynomu na kořenové činitele, jsou voleny speciálně tak, aby kořeny šlo nějakým trikem nalézt. Zde uvedená věta říká, že tyto triky nemohou být univerzálními postupy pro hledání rozkladu jakéhokoli polynomu.

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

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

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

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

(1) $\boldsymbol{x} + \boldsymbol{o} = \boldsymbol{x} \qquad \forall\, \boldsymbol{x} \in L$

(2) $\alpha \cdot \boldsymbol{o} = \boldsymbol{o} \qquad \forall\, \alpha \in \mathbf{R}$

(3) Nechť $\boldsymbol{x} \in L$. Je-li $\alpha \cdot \boldsymbol{x} = \boldsymbol{o}$ a $\alpha \neq 0$, pak $\boldsymbol{x} = \boldsymbol{o}$.

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

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

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

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

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

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

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

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

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

2.5 **Definice.** *Triviální* lineární kombinace vektorů $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ je taková lineární kombinace, která má všechny koeficienty nulové, tj.

$$0\boldsymbol{x}_1 + 0\boldsymbol{x}_2 + \cdots + 0\boldsymbol{x}_n.$$

Netriviální lineární kombinace je taková lineární kombinace, která není triviální, tj. aspoň jeden její koeficient je nenulový.

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

Poznámka. Vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou *lineárně závislé*, pokud existují reálná čísla $\alpha_1, \alpha_2, \ldots, \alpha_n$ tak, že aspoň jedno z nich je nenulové, a přitom platí

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

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

Poznámka. Vektory jsou *lineárně nezávislé*, pokud neexistuje netriviální lineární kombinace těchto vektorů, která je rovna nulovému vektoru.

Jinak: Vektory jsou *lineárně nezávislé*, pokud jedině triviální lineární kombinace je rovna nulovému vektoru.

Jinak: Vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou *lineárně nezávislé*, pokud z předpokladu

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

nutně plyne, že $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

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

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

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

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

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

Prázdnou množinu považujeme vždy za lineárně nezávislou.

Poznámka. Neprázdná konečná množina vektorů $K = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_n\}$ se nazývá *lineárně nezávislá*, pokud jsou vektory $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_n$ lineárně nezávislé.
Nekonečná množina vektorů $M \subseteq L$ se nazývá *lineárně nezávislá*, pokud všechny konečné podmnožiny $K \subseteq M$ jsou lineárně nezávislé.

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

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

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

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

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

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

(1) $M \subseteq \langle M \rangle$

(2) $\langle M \rangle = \langle \langle M \rangle \rangle$

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

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

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

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

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

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

(1) B je lineárně nezávislá

(2) $\langle B \rangle = L$

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

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

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

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

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

2.59 **Věta.** Nechť B_1 a B_2 jsou dvě báze stejného lineárního prostoru L. Pak jsou buď obě nekonečné, nebo mají obě stejný počet prvků.

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

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

2.64 **Věta.** Nechť L je lineární prostor, $\dim L = n$ a $M = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m\}$. Pak platí:

(1) Je-li M lineárně nezávislá, pak $m \le n$.

(2) Je-li $m > n$, pak M je lineárně závislá.

(3) Nechť $m = n$. Pak M je lineárně nezávislá právě tehdy, když $\langle M \rangle = L$.

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

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

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

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

Nechť $\mathbf{A} = (a_{r,s}), r \in \{1,\ldots,m\}, s \in \{1,\ldots,n\}$. Uspořádanou m-tici reálných čísel $(a_{1,s}, a_{2,s}, \ldots, a_{m,s})$ nazýváme *s-tým sloupcem matice* $\mathbf{A}$.
Matici typu (m,n), která má všechny prvky nulové, nazýváme *nulovou maticí*.
Matici typu (m,n) nazýváme *čtvercovou maticí*, pokud $m = n$.

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

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

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

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

3.9 **Definice.** Symbolem $\mathbf{A} \sim \mathbf{B}$ označujeme skutečnost, že matice $\mathbf{B}$ vznikla z matice $\mathbf{A}$ konečným počtem kroků podle Gaussovy eliminační metody.

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

3.12 **Definice.** Lineární obal množiny všech řádků matice $\mathbf{A}$ značíme $\langle \mathrm{r} \colon \mathbf{A} \rangle$.

3.13 **Věta.** Je-li $\mathbf{A} \sim \mathbf{B}$, pak $\langle \mathrm{r} \colon \mathbf{A} \rangle = \langle \mathrm{r} \colon \mathbf{B} \rangle$.

3.15 **Definice.** *Hodnost matice* **A** značíme hod(**A**) a definujeme hod(**A**) = dim⟨r: **A**⟩.

3.17 **Věta.** Je-li **A** ~ **B**, pak hod(**A**) = hod(**B**). Jinými slovy, Gaussova eliminační metoda nemění hodnost matice.

3.18 **Věta.** Hodnost matice je maximální počet lineárně nezávislých řádků matice. Přesněji řečeno, jedná se o počet prvků takové množiny řádků, která je nejpočetnější, a přitom lineárně nezávislá.

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

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

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

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

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

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

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

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

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

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

(1) $(\mathbf{A} \cdot \mathbf{B}) \cdot \mathbf{C} = \mathbf{A} \cdot (\mathbf{B} \cdot \mathbf{C})$,

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

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

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

(5) $(\mathbf{A} \cdot \mathbf{B})^T = \mathbf{B}^T \cdot \mathbf{A}^T$

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

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

3.48 **Definice.** Nechť $\mathbf{A}$ je čtvercová matice typu (n, n) a $\mathbf{E}$ je jednotková matice stejného typu. Matici $\mathbf{B}$ typu (n, n), která splňuje vlastnost

$$\mathbf{A} \cdot \mathbf{B} = \mathbf{E} = \mathbf{B} \cdot \mathbf{A}$$

nazýváme *inverzní maticí* k matici $\mathbf{A}$. Inverzní matici k matici $\mathbf{A}$ označujeme symbolem $\mathbf{A}^{-1}$.

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

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

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

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

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

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

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

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

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

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

4.5 **Definice.** Nechť $(i_1, i_2, \dots, i_n)$ je permutace n prvků. *Počet inverzí* této permutace je počet takových dvojic (i_k, i_l), pro které platí $i_k > i_l$, a přitom $k < l$.

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

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

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

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

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

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

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

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

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

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

4.21 **Věta.** Základní vlastnosti determinantu.
(V1) Jestliže se matice $\mathbf{B}$ liší od matice $\mathbf{A}$ jen prohozením jedné dvojice řádků, pak $\det \mathbf{B} = -\det \mathbf{A}$.
(V2) Jestliže matice $\mathbf{A}$ má dva stejné řádky, pak $\det \mathbf{A} = 0$.
V dalších vlastnostech (V3) až (V5) označujeme symbolem $\begin{pmatrix} \vdots \\ \boldsymbol{a}_i \\ \vdots \end{pmatrix}$ matice, které se liší pouze v i-tém řádku, zde označeném $\boldsymbol{a}_i$. V řádcích, které jsou vyznačeny tečkami, se jednotlivé matice shodují.

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

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

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

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

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

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

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

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

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

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

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

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

4.38 **Věta.** Nechť $\mathbf{A}$ je regulární matice. Pak $\det \mathbf{A}^{-1} = 1/\det \mathbf{A}$.

5.1 **Definice.** Nechť $\mathbf{A}$ je matice reálných čísel typu (m,n), nechť dále $\boldsymbol{x}$ je jednosloupcová matice symbolů $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ typu $(n,1)$ a $\boldsymbol{b}$ je matice reálných čísel $\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ typu $(m,1)$. Pak maticovou rovnost

$$\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$$

navýváme *soustavou m lineárních rovnic o n neznámých*. Matici $\mathbf{A}$ nazýváme *maticí soutavy* a vektor $\boldsymbol{b}^T = (b_1,\dots,b_m)$ nazýváme *vektorem pravých stran*. Připíšeme-li k matici soustavy do dalšího sloupce matici $\boldsymbol{b}$ oddělenou (pouze pro přehlednost) svislou čarou, dostáváme matici $(\mathbf{A}|\boldsymbol{b})$ typu $(m, n+1)$, kterou nazýváme *rozšířenou maticí soustavy*.

5.2 **Definice.** *Řešením soustavy* $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ je takový vektor

$$\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbf{R}^n,$$

pro který platí: dosadíme-li hodnoty α_i za symboly x_i, pak je splněna požadovaná maticová rovnost, tj.

$$\mathbf{A} \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}.$$

Řešit soustavu $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ znamená nalézt všechna její řešení, tj. nalézt podmnožinu $\mathbf{R}^n$ všech řešení této soustavy.

5.4 **Věta.** (Frobeniova). Soustava $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ má řešení právě tehdy, když

$$\operatorname{hod} \mathbf{A} = \operatorname{hod}(\mathbf{A}|\boldsymbol{b}),$$

tj. když hodnost matice soustavy se rovná hodnosti rozšířené matice soustavy.

5.6 **Definice.** Nechť $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ je soustava m lineárních rovnic o n neznámých a $\mathbf{C}\boldsymbol{x} = \boldsymbol{d}$ je soustava k lineárních rovnic o stejném počtu n neznámých. Říkáme, že tyto soustavy jsou *ekvivalentní*, pokud obě soustavy mají stejné množiny řešení.

5.8 **Věta.** Ke každé soustavě $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ lze nalézt ekvivalentní soustavu $\mathbf{C}\boldsymbol{x} = \boldsymbol{d}$, jejíž matice $\mathbf{C}$ je horní trojúhelníková.

5.9 **Definice.** Existuje-li v matici $\boldsymbol{b}$ aspoň jeden prvek nenulový, říkáme, že je soustava lineárních rovnic $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ *nehomogenní*. Jsou-li všechny prvky v matici $\boldsymbol{b}$ nulové, nazýváme soustavu rovnic *homogenní* a zapisujeme ji takto:

$\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$ (symbolem $\boldsymbol{o}$ nyní značíme jednosloupcovou nulovou matici).

5.10 **Věta.** Množina všech řešení homogenní soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$ s n neznámými tvoří lineární podprostor lineárního prostoru $\mathbf{R}^n$.

5.13 **Věta.** Nechť $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$ je homogenní soustava lineárních rovnic o n neznámých, $k = n - \operatorname{hod} \mathbf{A}$. Pak existuje k lineárně nezávislých vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ z $\mathbf{R}^n$ takových, že pro množinu M_0 všech řešení soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$ platí

$$M_0 = \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \rangle.$$

Vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ tvoří jednu z možných bází lineárního prostoru všech řešení M_0.

5.14 **Věta.** Nechť M_0 je lineární prostor všech řešení homogenní soustavy lineárních rovnic $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$ s n neznámými. Pak $\dim M_0 = n - \operatorname{hod}\mathbf{A}$.

5.17 **Definice.** Nechť $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ je nehomogenní soustava lineárních rovnic o n neznámých a $\boldsymbol{v} \in \mathbf{R}^n$ je nějaké jedno její řešení. Takovému řešení $\boldsymbol{v}$ říkáme *partikulární řešení* nehomogenní soustavy.
Pokud zaměníme matici $\boldsymbol{b}$ za nulovou matici stejného typu, dostáváme homogenní soustavu $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$, kterou nazýváme *přidruženou homogenní soustavou* k soustavě $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$.

5.18 **Věta.** (1) Nechť $\boldsymbol{v}$ je partikulární řešení nehomogenní soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ a $\boldsymbol{u}$ je libovolné řešení přidružené homogenní soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$. Pak $\boldsymbol{v} + \boldsymbol{u}$ je také řešením soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$.
(2) Nechť $\boldsymbol{v}$ a $\boldsymbol{w}$ jsou dvě partikulární řešení nehomogenní soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$. Pak $\boldsymbol{v} - \boldsymbol{w}$ je řešením přidružené homogenní soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$.

5.19 **Věta.** Nechť $\boldsymbol{v}$ je partikulární řešení soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ a M_0 je lineární prostor všech řešení přidružené homogenní soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$. Pak pro množinu M všech řešení soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ platí

$$M = \{\boldsymbol{v} + \boldsymbol{u};\ \ \boldsymbol{u} \in M_0\}.$$

5.29 **Věta.** (Cramerovo pravidlo). Nechť $\mathbf{A}$ je regulární čtvercová matice. Pak pro i-tou složku řešení soustavy $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ platí

$$\alpha_i = \frac{\det \mathbf{B}_i}{\det \mathbf{A}},$$

kde matice $\mathbf{B}_i$ je shodná s maticí $\mathbf{A}$ až na i-tý sloupec, který je zaměněn za sloupec pravých stran.

5.34 **Věta.** Nechť homogenní soustava lineárních rovnic $\mathbf{A}\boldsymbol{x} = \boldsymbol{o}$ má matici soustavy ve tvaru

$$\mathbf{A} = (\mathbf{E}|\mathbf{C}),$$

kde $\mathbf{E}$ je jednotková matice typu (m,m) a $\mathbf{C}$ je libovolná matice typu (m,k). Pak existuje báze řešení této soustavy $\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_k$, která má tvar:

$$\begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \\ \vdots \\ \boldsymbol{b}_k \end{pmatrix} = (-\mathbf{C}^T|\mathbf{E}'),$$

kde $\mathbf{E}'$ je jednotková matice typu (k,k).

5.39 **Věta.** Nechť $\mathbf{A}$ je reulární matice a $\mathbf{B}$ je libovolná matice se stejným počtem řádků. Rovnost $\mathbf{A} \cdot \mathbf{X} = \mathbf{B}$ je ekvivalentní s $(\mathbf{A}|\mathbf{B}) \sim (\mathbf{E}|\mathbf{X})$.

6.3 **Definice.** Nechť L je lineární prostor, M a N jsou jeho podprostory. Množinu $\langle M \cup N \rangle$ nazýváme *spojením podprostorů M a N* a značíme $M \vee N$.

6.5 **Věta.** Nechť L je lineární prostor, M a N jsou jeho podprostory. Pro podprostor $M \vee N$ platí:

$$M \vee N = \{\boldsymbol{y} + \boldsymbol{z};\ \boldsymbol{y} \in M, \boldsymbol{z} \in N\}.$$

6.6 **Věta.** Nechť L je lineární prostor konečné dimenze, M a N jsou jeho podprostory. Pak

$$\dim M + \dim N = \dim(M \cap N) + \dim(M \vee N)$$

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

6.10 **Definice.** Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je uspořádaná báze lineárního prostoru L a $\boldsymbol{x} \in L$ je libovolný vektor. Uspořádanou n-tici reálných čísel $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ nazýváme *souřadnicemi vektoru* $\boldsymbol{x}$ *vzhledem k uspořádané bázi* (B), pokud platí

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

Skutečnost, že $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ jsou souřadnice vektoru $\boldsymbol{x}$ vzhledem k uspořádané bázi (B) budeme zapisovat takto:

$$\boldsymbol{x} = (\alpha_1, \alpha_2, \ldots, \alpha_n)_{(B)}$$

6.12 **Věta.** Nechť (B) je uspořádaná báze lineárního porostoru L. Pak pro každý prvek $\boldsymbol{x} \in L$ jsou souřadnice $\boldsymbol{x}$ vzhledem k bázi (B) určeny jednoznačně.

6.13 **Věta.** Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je uspořádaná báze lineárního prostoru L. Pak pro každý prvek $\boldsymbol{a} \in \mathbf{R}^n$, $\boldsymbol{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, existuje $\boldsymbol{x} \in L$ takový, že $\boldsymbol{x} = (\alpha_1, \alpha_2, \ldots, \alpha_n)_{(B)}$.

6.18 **Definice.** Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ a $(C) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n)$ jsou dvě uspořádané báze stejného lineárního prostoru L. Matici $\mathbf{A}$, která splňuje maticovou rovnost

$$(\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n) \cdot \mathbf{A} = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n)$$

nazýváme *maticí přechodu od uspořádané báze (B) k uspořádané bázi (C)*.
Na definiční rovnost se díváme jako na součin jednořádkové matice vektorů $(\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ s maticí $\mathbf{A}$ reálných čísel typu (n, n), který se má rovnat jednořádkové matici vektorů $(\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n)$.
Matici přechodu od báze (B) k bázi (C) budeme často pro názornost označovat $\mathbf{A}_{(B,C)}$.

6.19 **Věta.** Pro každé dvě uspořádané báze stejného lineárního prostoru (B) a (C) existuje právě jedna regulární matice přechodu $\mathbf{A}_{(B,C)}$.

6.21 **Věta.** Je-li $\mathbf{A}$ matice přechodu od báze (B) k bázi (C), pak $\mathbf{A}^{-1}$ je matice přechodu od báze (C) k bázi (B).

6.23 **Věta.** Nechť (B) a (C) jsou dvě uspořádané báze lineárního prostoru L, $\mathbf{A}_{(B,C)}$ je matice přechodu od (B) k (C). Pak pro souřadnice každého vektoru $\boldsymbol{x} \in L$, $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)_{(B)} = (y_1, y_2, \ldots, y_n)_{(C)}$ platí:

$$\mathbf{A}_{(B,C)} \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

6.27 **Věta.** Nechť $\mathbf{A}_{(B,C)}$ je matice přechodu od báze (B) k bázi (C) a $\mathbf{A}_{(C,D)}$ je matice přechodu od báze (C) k bázi (D). Pak pro matici přechodu $\mathbf{A}_{(B,D)}$ od báze (B) k bázi (D) platí

$$\mathbf{A}_{(B,D)} = \mathbf{A}_{(B,C)} \cdot \mathbf{A}_{(C,D)}$$

6.29 **Věta.** Nechť $\boldsymbol{a} \in \mathbf{R}^n$, $\boldsymbol{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Složky $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ jsou souřadnicemi vektoru $\boldsymbol{a}$ vzhledem ke standardní bázi (S):

$$(S) = ((1, 0, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, 0, 0, \ldots, 1)).$$

6.30 **Věta.** Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je uspořádaná báze lineárního prostoru $\mathbf{R}^n$. Matice přechodu od standardní báze (S) k bázi (B) má tvar

$$\mathbf{A}_{(S,B)} = (\boldsymbol{b}_1^T, \boldsymbol{b}_2^T, \ldots, \boldsymbol{b}_n^T)$$

kde symbolem $\boldsymbol{b}_i^T$ značíme sloupec složek vektoru $\boldsymbol{b}_i$. Jinými slovy, uvedenou matici přechodu sestavíme tak, že zapíšeme jednotlivé vektory báze vedle sebe, složky těchto vektorů zapíšeme do sloupců.

6.31 **Věta.** Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ a $(C) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n)$ jsou uspořádané báze lineárního prostoru $\mathbf{R}^n$. Pak pro matice přechodu $\mathbf{A}_{(B,C)}$ a $\mathbf{A}_{(C,B)}$ platí

$$(\mathbf{A}_{(C,B)} \,|\, \mathbf{E}) \sim (\boldsymbol{b}_1^T, \boldsymbol{b}_2^T, \ldots \boldsymbol{b}_n^T \,|\, \boldsymbol{c}_1^T, \boldsymbol{c}_2^T, \ldots \boldsymbol{c}_n^T) \sim (\mathbf{E} \,|\, \mathbf{A}_{(B,C)}),$$

kde „~“ značí konečně mnoho kroků Gaussovy eliminační metody, $\mathbf{E}$ je jednotková matice a $\boldsymbol{b}_i^T$ resp. $\boldsymbol{c}_j^T$ jsou vektory $\boldsymbol{b}_i$ resp. $\boldsymbol{c}_j$, jejichž složky jsou zapsány do sloupců.

7.2 **Definice.** Nechť L_1 a L_2 jsou libovolné množiny. *Zobrazením $\mathcal{A}$ z množiny L_1 do množiny L_2* rozumíme jakýkoli předpis, který každému prvku z množiny L_1 přiřadí jednoznačným způsobem nějaký prvek z množiny L_2. Skutečnost, že $\mathcal{A}$ je zobrazení z množiny L_1 do množiny L_2 zapisujeme $\mathcal{A} : L_1 \to L_2$.
Je-li $\boldsymbol{x} \in L_1$, pak zobrazení $\mathcal{A} : L_1 \to L_2$ přiřadí prvku $\boldsymbol{x}$ jednoznačně nějaký prvek z množiny L_2. Tento prvek označujeme symbolem $\mathcal{A}(\boldsymbol{x}) \in L_2$ a říkáme mu *hodnota zobrazení $\mathcal{A}$ v bodě $\boldsymbol{x}$*. Je-li $M \subseteq L_1$, pak definujeme

$$\mathcal{A}(M) = \{\boldsymbol{y} \in L_2;\ \exists \boldsymbol{x} \in M,\ \mathcal{A}(\boldsymbol{x}) = \boldsymbol{y}\}.$$

7.3 **Definice.** Nechť L_1 a L_2 jsou libovolné množiny a uvažujme $\mathcal{A} : L_1 \to L_2$. Pokud platí $\mathcal{A}(L_1) = L_2$, říkáme, že $\mathcal{A}$ je zobrazení z množiny L_1 *na množinu L_2*.

7.5 **Definice.** Nechť L_1 a L_2 jsou libovolné množiny a uvažujme $\mathcal{A} : L_1 \to L_2$. Zobrazení $\mathcal{A}$ je *prosté*, pokud pro každé dva prvky $\boldsymbol{x}_1 \in L_1, \boldsymbol{x}_2 \in L_1, \boldsymbol{x}_1 \neq \boldsymbol{x}_2$ platí $\mathcal{A}(\boldsymbol{x}_1) \neq \mathcal{A}(\boldsymbol{x}_2)$.

7.6 **Definice.** Nechť L_1 a L_2 jsou lineární prostory, $\mathcal{A} : L_1 \to L_2$ je zobrazení z L_1 do L_2. Zobrazení $\mathcal{A}$ nazýváme *lineárním zobrazením*, pokud pro všechna $\boldsymbol{x} \in L_1$, $\boldsymbol{y} \in L_1$, $\alpha \in \mathbf{R}$ platí

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

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

7.8 **Věta.** (Princip superpozice). Nechť L_1 a L_2 jsou lineární prostory. Zobrazení $\mathcal{A} : L_1 \to L_2$ je lineární právě tehdy, když pro všechna $\boldsymbol{x} \in L_1$, $\boldsymbol{y} \in L_1$, $\alpha \in \mathbf{R}$, $\beta \in \mathbf{R}$ platí

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

7.10 **Věta.** Pro lineární zobrazení $\mathcal{A} : L_1 \to L_2$ platí $\mathcal{A}(\boldsymbol{o}_1) = \boldsymbol{o}_2$, kde $\boldsymbol{o}_1$ je nulový vektor lineárního prostoru L_1 a $\boldsymbol{o}_2$ je nulový vektor lineárního prostoru L_2.

7.14 **Věta.** Nechť $\mathcal{A} : L_1 \to L_2$ je lineární zobrazení, $M \subseteq L_1$. Pak $\mathcal{A}(\langle M \rangle) = \langle \mathcal{A}(M) \rangle$.

7.16 **Definice.** Nechť L_1, L_2 jsou lineární prostory, $\boldsymbol{o}_2$ je nulový vektor v lineárním prostoru L_2 a $\mathcal{A} : L_1 \to L_2$ je lineární zobrazení. Množinu

$$\operatorname{Ker} \mathcal{A} = \{\boldsymbol{x} \in L_1;\ \mathcal{A}(\boldsymbol{x}) = \boldsymbol{o}_2\}$$

nazýváme *jádrem lineárního zobrazení $\mathcal{A}$.*

7.19 **Věta.** Jádro lineárního zobrazení $\mathcal{A} : L_1 \to L_2$ tvoří lineární podprostor lineárního prostoru L_1.

7.20 **Věta.** Množina $\mathcal{A}(L_1)$ všech hodnot lineárního zobrazení $\mathcal{A} : L_1 \to L_2$ tvoří lineární podprostor lineárního prostoru L_2.

7.21 **Definice.** *Defekt lineárního zobrazení* $\mathcal{A} : L_1 \to L_2$ je definován, jako $\dim \operatorname{Ker} \mathcal{A}$ a *hodnost lineárního zobrazení* $\mathcal{A}$ je definována jako $\dim \mathcal{A}(L_1)$. Defekt $\mathcal{A}$ značíme $\operatorname{def} \mathcal{A}$ a hodnost $\mathcal{A}$ značíme $\operatorname{hod} \mathcal{A}$. Je tedy

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

7.27 **Věta.** Nechť $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ je báze lineárního prostoru L_1 a nechť jsou dány libovolné vektory $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_n$ z lineárního prostoru L_2. Pak existuje právě jedno lineární zobrazení $\mathcal{A} : L_1 \to L_2$, pro které platí

$$\mathcal{A}(\boldsymbol{b}_i) = \boldsymbol{y}_i, \quad \forall i \in \{1, 2, \ldots, n\}$$

7.29 **Věta.** Nechť $\mathcal{A} : L_1 \to L_2$ je lineární zobrazení. Pak platí:
(1) Jsou-li $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ lineárně závislé vektory v L_1, pak jsou i vektory $\mathcal{A}(\boldsymbol{x}_1), \mathcal{A}(\boldsymbol{x}_2), \ldots, \mathcal{A}(\boldsymbol{x}_n)$ lineárně závislé v L_2.
(2) Jsou-li $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ lineárně nezávislé vektory v L_1, pak vektory $\mathcal{A}(\boldsymbol{x}_1), \mathcal{A}(\boldsymbol{x}_2), \ldots, \mathcal{A}(\boldsymbol{x}_n)$ v L_2 nemusí být lineárně nezávislé.

7.30 **Věta.** Nechť $\mathcal{A} : L_1 \to L_2$ je lineární zobrazení. Následující podmínky jsou ekvivalentní:
(1) $\mathcal{A}$ je prosté.
(2) $\operatorname{def} \mathcal{A} = 0$.
(3) Jsou-li $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ lineárně nezávislé, jsou lineárně nezávislé i vektory $\mathcal{A}(\boldsymbol{x}_1), \mathcal{A}(\boldsymbol{x}_2), \ldots, \mathcal{A}(\boldsymbol{x}_n)$.

7.31 **Definice.** Nechť $\mathcal{A} : L_1 \to L_2$ a $\mathcal{B} : L_2 \to L_3$ jsou zobrazení. Symbolem $\mathcal{B} \circ \mathcal{A} : L_1 \to L_3$ označujeme *složené zobrazení*, které je definováno předpisem $(\mathcal{B} \circ \mathcal{A})(\boldsymbol{x}) = \mathcal{B}(\mathcal{A}(\boldsymbol{x}))$, $\forall \boldsymbol{x} \in L_1$.

7.32 **Věta.** Nechť $\mathcal{A} : L_1 \to L_2$ a $\mathcal{B} : L_2 \to L_3$ jsou lineární zobrazení. Pak je lineární též složené zobrazení $\mathcal{B} \circ \mathcal{A} : L_1 \to L_3$.

7.33 **Definice.** *Identické zobrazení* je zobrazení $\mathcal{I} : L \to L$, které je definováno předpisem $\mathcal{I}(\boldsymbol{x}) = \boldsymbol{x}$. Stručně nazýváme zobrazení $\mathcal{I}$ *identitou*.
Nechť $\mathcal{A} : L_1 \to L_2$ je prosté zobrazení. Pak definujeme *inverzní zobrazení* $\mathcal{A}^{-1} : \mathcal{A}(L_1) \to L_1$ jako takové zobrazení, které splňuje $\mathcal{A}^{-1} \circ \mathcal{A} = \mathcal{I}$, kde $\mathcal{I} : L_1 \to L_1$ je identita.

7.34 **Věta.** Je-li $\mathcal{A} : L_1 \to L_2$ prosté, pak existuje právě jedno inverzní zobrazení $\mathcal{A}^{-1} : \mathcal{A}(L_1) \to L_1$.

7.35 **Věta.** Je-li L lineární prostor, pak identita $\mathcal{I} : L \to L$ je lineární. Je-li $\mathcal{A} : L_1 \to L_2$ lineární a prosté zobrazení, pak též $\mathcal{A}^{-1} : \mathcal{A}(L_1) \to L_1$ je lineární.

7.36 **Věta.** Nechť $\mathcal{A} : L_1 \to L_2$ je lineární, prosté a „na“ L_2. Pak je inverzní zobrazení $\mathcal{A}^{-1} : L_2 \to L_1$ rovněž lineární, prosté a „na“ L_1.

7.37 **Definice.** Zobrazení $\mathcal{A} : L_1 \to L_2$ nazýváme *izomorfismus*, pokud je lineární, prosté a „na“ L_2.

Lineární prostor L_1 nazýváme *izomorfní s* L_2, pokud existuje izomorfismus $\mathcal{A} : L_1 \to L_2$. Protože k prostému lineárnímu zobrazení, které je „na“ L_2, existuje inverzní zobrazení $\mathcal{A}^{-1} : L_2 \to L_1$, které je podle věty 7.36 rovněž izomorfismem, platí: je-li L_1 izomorfní s L_2, je též L_2 izomorfní s L_1. Často proto říkáme, že L_1 a L_2 jsou (vzájemně) izomorfní.

7.39 **Věta.** Každý lineární prostor L, pro který je $\dim L = n$, je izomorfní s lineárním prostorem $\mathbf{R}^n$.

7.41 **Věta.** Nechť $\mathcal{A} : L_1 \to L_2$ a $\mathcal{B} : L_2 \to L_3$ jsou izomorfismy. Pak je izomorfismem i složené zobrazení $\mathcal{B} \circ \mathcal{A} : L_1 \to L_3$.

7.42 **Věta.** Dva lineární prostory konečné dimenze jsou izomorfní právě tehdy, když se rovnají jejich dimenze.

7.43 **Definice.** Nechť L_1 a L_2 jsou lineární prostory konečné dimenze, $\mathcal{A} : L_1 \to L_2$ je lineární. Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je uspořádaná báze L_1 a $(C) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m)$ je uspořádaná báze L_2. Matici $\mathbf{A}$ typu (m,n), která splňuje maticovou rovnost

$$(\mathcal{A}(\boldsymbol{b}_1), \mathcal{A}(\boldsymbol{b}_2), \ldots, \mathcal{A}(\boldsymbol{b}_n)) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m) \cdot \mathbf{A}$$

nazýváme *maticí zobrazení $\mathcal{A}$ vzhledem k uspořádaným bázím (B) a (C)*. Na definiční rovnost se díváme jako na součin jednořádkové matice vektorů $(\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m)$ s maticí $\mathbf{A}$ reálných čísel typu (m,n), který se má rovnat jednořádkové matici vektorů $(\mathcal{A}(\boldsymbol{b}_1), \mathcal{A}(\boldsymbol{b}_2), \ldots, \mathcal{A}(\boldsymbol{b}_m))$

7.44 **Věta.** Nechť platí předpoklady z definice 7.43. Pak matice $\mathbf{A}$ zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C) existuje a je určena jednoznačně.

7.45 **Věta.** Nechť L_1, L_2 jsou lineární prostory konečné dimenze, $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n)$ je uspořádaná báze L_1 a $(C) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \dots, \boldsymbol{c}_m)$ je uspořádaná báze L_2. Pak ke každé matici $\mathbf{A}$ typu (m, n) existuje právě jedno lineární zobrazení $\mathcal{A} : L_1 \to L_2$ takové, že $\mathbf{A}$ je maticí zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C).

7.48 **Věta.** Nechť (B) je báze v L_1, (C) je báze v L_2, $\mathcal{A} : L_1 \to L_2$ je lineární a $\mathbf{A}$ je maticí zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C). Pak $\operatorname{hod} \mathbf{A} = \operatorname{hod} \mathcal{A}$.

7.49 **Věta.** Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n)$ je báze v L_1, $(C) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \dots, \boldsymbol{c}_m)$ je báze v L_2, $\mathcal{A} : L_1 \to L_2$ je lineární a $\mathbf{A}$ je maticí zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C). Pak pro každý vektor $\boldsymbol{x} \in L_1$, $\boldsymbol{x} = (x_1, x_2, \dots, x_n)_{(B)}$, platí pro souřadnice vektoru $\mathcal{A}(\boldsymbol{x}) = (y_1, y_2, \dots, y_m)_{(C)}$ následující vzorec:

$$\mathbf{A} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}$$

7.53 **Věta.** Nechť L_1, L_2 jsou lineární prostory konečné dimenze, $\mathcal{A} : L_1 \to L_2$ je lineární. Pak

$$\operatorname{def} \mathcal{A} + \operatorname{hod} \mathcal{A} = \dim L_1.$$

7.55 **Věta.** Nechť L_1, L_2, L_3 jsou lineární prostory konečné dimenze, $\mathcal{A} : L_1 \to L_2$, $\mathcal{B} : L_2 \to L_3$ jsou lineární zobrazení. Nechť dále (B) je uspořádaná báze L_1, (C) je uspořádaná báze L_2 a (D) je uspořádaná báze L_3. Předpokládejme ještě, že $\mathbf{A}$ je matice zobrazení $\mathcal{A}$ vzhledem k bázím (B) a (C) a konečně $\mathbf{B}$ je matice zobrazení $\mathcal{B}$ vzhledem k bázím (C) a (D). Pak $\mathbf{B} \cdot \mathbf{A}$ je matice složeného zobrazení $\mathcal{B} \circ \mathcal{A}$ vzhledem k bázím (B) a (D).

7.56 **Věta.** Nechť (B) a (C) jsou dvě báze lineárního prostoru L. Pak matice identického zobrazení $\mathcal{I} : L \to L$ vzhledem k bázím (B) a (C) je rovna matici přechodu $\mathbf{A}_{(C,B)}$ od báze (C) k bázi (B).

7.59 **Věta.** Nechť $\mathcal{A} : L_1 \to L_2$ je lineární zobrazení a nechť (B_1), (C_1) jsou báze lineárního prostoru L_1 a (B_2), (C_2) jsou báze lineárního prostoru L_2. Označme symbolem $\mathbf{A}_{(B_1,C_1)}$ matici přechodu od báze (B_1) k (C_1) a $\mathbf{A}_{(C_2,B_2)}$ matici přechodu od báze (C_2) k (B_2). Je-li $\mathbf{A}$ matice zobrazení $\mathcal{A}$ vzhledem k bázím (B_1), (B_2), pak $\mathbf{A}_{(C_2,B_2)} \cdot \mathbf{A} \cdot \mathbf{A}_{(B_1,C_1)}$ je matice téhož lineárního zobrazení vzhledem k bázím (C_1), (C_2).

7.60 **Definice.** Nechť $\mathcal{A} : L \to L$ je lineární zobrazení (lineární prostor vzorů i obrazů je stejný a má konečnou dimenzi). Místo, abychom mluvili o matici lineárního zobrazení vzhledem ke stejným bázím (B) a (B) (to působí, jako bychom koktali), stručně se zmiňujeme o *matici zobrazení $\mathcal{A}$ vzhledem k bázi* (B).

7.61 **Věta.** Nechť $\mathcal{A} : L \to L$ je lineární zobrazení, (B), (C) jsou dvě báze lineárního prostoru L a $\mathbf{A}_{(B,C)}$ je matice přechodu od báze (B) k bázi (C). Je-li $\mathbf{A}$ matice zobrazení $\mathcal{A}$ vzhledem k bázi (B), pak $\mathbf{A}_{(B,C)}^{-1} \cdot \mathbf{A} \cdot \mathbf{A}_{(B,C)}$ je maticí téhož lineárního zobrazení vzhledem k bázi (C).

7.63 **Definice.** Matice $\mathbf{A}$ je *podobná* matici $\mathbf{B}$, pokud existuje regulární matice $\mathbf{P}$ taková, že platí $\mathbf{B} = \mathbf{P}^{-1} \cdot \mathbf{A} \cdot \mathbf{P}$.

7.66 **Definice.** Nechť $\mathcal{A} : L \to L$ je lineární zobrazení. Číslo $\lambda \in \mathbf{C}$ se nazývá *vlastním číslem zobrazení* $\mathcal{A}$, pokud existuje vektor $\boldsymbol{x} \in L$, $\boldsymbol{x} \neq \boldsymbol{o}$ takový, že $\mathcal{A}(\boldsymbol{x}) = \lambda\, \boldsymbol{x}$. Vektor $\boldsymbol{x}$, který splňuje uvedenou rovnost, se nazývá *vlastní vektor zobrazení* $\mathcal{A}$ *příslušný vlastnímu číslu* λ.

7.70 **Definice.** Nechť $\mathbf{A}$ je čtvercová matice typu (n, n) reálných nebo komplexních čísel. Číslo $\lambda \in \mathbf{C}$ se nazývá *vlastním číslem matice* $\mathbf{A}$, pokud existuje $\boldsymbol{x} \in \mathbf{C}^n$, $\boldsymbol{x} \neq \boldsymbol{o}$ takový, že $\mathbf{A} \cdot \boldsymbol{x}^T = \lambda\, \boldsymbol{x}^T$. Vektor $\boldsymbol{x}$, který splňuje uvedenou rovnost, se nazývá *vlastní vektor matice* $\mathbf{A}$ *příslušný vlastnímu číslu* λ.

7.71 **Věta.** Nechť $\mathcal{A} : L \to L$ je lineární zobrazení a $\mathbf{A}$ je jeho matice vzhledem k nějaké bázi (B). Pak λ je vlastním číslem zobrazení $\mathcal{A}$ právě tehdy, když je vlastním číslem matice $\mathbf{A}$. Navíc $\boldsymbol{x}$ je vlastní vektor zobrazení $\mathcal{A}$ příslušný λ právě tehdy, když souřadnice vektoru $\boldsymbol{x}$ vzhledem k bázi (B) tvoří vlastní vektor matice $\mathbf{A}$ příslušný λ.

7.75 **Definice.** Nechť $\mathbf{A}$ je čtvercová matice. Polynom $\det(\mathbf{A} - \lambda\,\mathbf{E})$ nazýváme *charakteristický polynom matice* $\mathbf{A}$ a rovnost $\det(\mathbf{A} - \lambda\,\mathbf{E}) = 0$ charakteristickou rovnicí. Je-li λ k-násobným kořenem charakteristické rovnice, říkáme, že λ je *k-násobným vlastním číslem*.

7.78 **Věta.** Podobné matice mají stejný charakteristický polynom.

7.82 **Věta.** Nechť $\mathbf{A}$ je čtvercová matice typu (n, n). Sestavme libovolná komplexní čísla $\lambda_1, \ldots, \lambda_n$ do diagonální matice $\mathbf{D} = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ a libovolné nenulové vektory $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ z $\mathbf{C}^n$ zapišme do sloupců matice $\mathbf{P}$, tj. $\mathbf{P} = (\boldsymbol{x}_1^T, \ldots, \boldsymbol{x}_n^T)$. Pak platí: čísla $\lambda_1, \ldots, \lambda_n$ jsou vlastními čísly matice $\mathbf{A}$ a $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ jsou jejich odpovídající vlastní vektory právě tehdy, když je splněna rovnost $\mathbf{PD} = \mathbf{AP}$.

7.83 **Věta.** Nechť má čtvercová matice **A** s n řádky n lineárně nezávislých vlastních vektorů (každý z nich přísluší nějakému vlastnímu číslu matice). Pak je matice **A** podobná diagonální matici.

7.84 **Věta.** Nechť je matice **A** podobná s diagonální maticí, tj. existuje regulární matice **P** a diagonální matice **D** takové, že $\mathbf{A} = \mathbf{P}\mathbf{D}\mathbf{P}^{-1}$. Pak **D** obsahuje vlastní čísla matice **A** a ve sloupcích matice **P** jsou vlastní vektory příslušné (podle pořadí) odpovídajícím vlastním číslům zapsaným v **D**.

7.87 **Věta.** Vlastní vektory, které příslušejí vzájmeně různým vlastním číslům, jsou lineárně nezávislé.

7.92 **Věta.** Nechť $\mathcal{A} : L \to L$ je lineární zobrazení, $\dim L = n$. Zobrazení $\mathcal{A}$ má n lineárně nezávislých vlastních vektorů právě tehdy, když existuje báze (B) prostoru L taková, že $\mathcal{A}$ má vzhledem k této bázi diagonální matici **D**. Přitom na diagonále matice **D** jsou vlastní čísla zobrazení $\mathcal{A}$ a báze (B) obsahuje vlastní vektory příslušné vlastním číslům v matici **D** ve stejném pořadí.

8.2 **Definice.** Nechť L je lineární prostor. Operaci $\cdot : L \times L \to \mathbf{R}$ nazveme *skalárním součinem*, pokud splňuje $\forall \boldsymbol{x} \in L$, $\forall \boldsymbol{y} \in L$, $\forall \boldsymbol{z} \in L$, $\forall \alpha \in \mathbf{R}$ následující vlastnosti

(1) $\boldsymbol{x} \cdot \boldsymbol{y} = \boldsymbol{y} \cdot \boldsymbol{x}$

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

(3) $(\alpha \cdot \boldsymbol{x}) \cdot \boldsymbol{y} = \alpha \cdot (\boldsymbol{x} \cdot \boldsymbol{y})$

(4) $\boldsymbol{x} \cdot \boldsymbol{x} \geq 0, \quad \boldsymbol{x} \cdot \boldsymbol{x} = 0$ jen tehdy, když $\boldsymbol{x} = \boldsymbol{o}$

Ve vlastnosti (4) značí symbol $\boldsymbol{o}$ nulový vektor lineárního prostoru L.

8.6 **Věta.** Nechť L je lineární prostor se skalárním součinem, $\boldsymbol{o}$ je jeho nulový vektor. Pak pro všechna $\boldsymbol{x} \in L$, $\boldsymbol{y} \in L$ a $\boldsymbol{z} \in L$ platí: (1) $\boldsymbol{x} \cdot \boldsymbol{o} = \boldsymbol{o} \cdot \boldsymbol{x} = 0$, (2) $\boldsymbol{z} \cdot (\boldsymbol{x} + \boldsymbol{y}) = \boldsymbol{z}\boldsymbol{x} + \boldsymbol{z}\boldsymbol{y}$.

8.11 **Definice.** Čtvercová matice $\mathbf{A}$ typu (n, n) je *symetrická*, pokud platí $\mathbf{A}^T = \mathbf{A}$.

8.12 **Definice.** Nechť $\mathbf{A}$ je čtvercová matice typu (n, n). Označme $\mathbf{A}_i$ čtvercovou matici typu $(n - i, n - i)$, která vzniká z matice $\mathbf{A}$ vynecháním posledních i řádků a posledních i sloupců. Matice $\mathbf{A}$ se nazývá *pozitivně definitní*, pokud všechny determinanty $\det \mathbf{A}_i$, $i \in \{0, 1, 2, \ldots, n - 1\}$ jsou kladné.

8.14 **Věta.** Nechť $\mathbf{A}$ je čtevrcová matice typu (n, n). Definujme součin na $\mathbf{R}^n$ takto. Pro $\boldsymbol{x} \in \mathbf{R}^n$, $\boldsymbol{y} \in \mathbf{R}^n$ je

$$\boldsymbol{x} \cdot \boldsymbol{y} = \boldsymbol{x} \cdot \mathbf{A} \cdot \boldsymbol{y}^T,$$

kde na pravé straně rovnosti je maticový součin jednořádkové matice $\boldsymbol{x}$, která obsahuje složky vektoru $\boldsymbol{x}$, s maticí $\mathbf{A}$ a s maticí $\boldsymbol{y}^T$, což je sloupec složek vektoru $\boldsymbol{y}$.
Pak $\boldsymbol{x} \cdot \boldsymbol{y}$ je skalárním součinem právě tehdy, když $\mathbf{A}$ je symetrická a pozitivně definitní matice.

8.17 **Definice.** Nechť L je lineární prostor se skalárním součinem. Pro $\boldsymbol{x} \in L$ definujeme *velikost vektoru* $\boldsymbol{x}$ hodnotou $\sqrt{\boldsymbol{x} \cdot \boldsymbol{x}}$. Velikost vektoru $\boldsymbol{x}$ značíme $|\boldsymbol{x}|$, takže je

$$|\boldsymbol{x}| = \sqrt{\boldsymbol{x} \cdot \boldsymbol{x}}, \qquad \text{tj. } |\boldsymbol{x}|^2 = \boldsymbol{x} \cdot \boldsymbol{x}$$

8.19 **Věta.** Nechť $\boldsymbol{x}$ je prvkem lineárního prostoru se skalárním součinem, $\alpha \in \mathbf{R}$. Pak

$$|\alpha \boldsymbol{x}| = |\alpha| \cdot |\boldsymbol{x}|.$$

Zápis $|\alpha|$ zde značí absolutní hodnotu reálného čísla, ostatní symboly „| |“ znamenají velikosti vektorů.

8.20 **Definice.** Nechť L je lineární prostor se skalárním součinem a $\boldsymbol{x} \in L$, $\boldsymbol{y} \in L$, $\boldsymbol{x} \neq \boldsymbol{o}$, $\boldsymbol{y} \neq \boldsymbol{o}$. Pak *úhel mezi vektory $\boldsymbol{x}$ a $\boldsymbol{y}$* je takové číslo ϕ, pro které platí

$$\cos \phi = \frac{\boldsymbol{x} \cdot \boldsymbol{y}}{|\boldsymbol{x}| \cdot |\boldsymbol{y}|}$$

8.22 **Věta.** (Schwartzova nerovnost). Nechť L je lineární prostor se skalárním součinem a $\boldsymbol{x} \in L$, $\boldsymbol{y} \in L$. Pak platí:

$$|\boldsymbol{x} \cdot \boldsymbol{y}| \le |\boldsymbol{x}| \cdot |\boldsymbol{y}|.$$

Symbol „| |“ na levé straně nerovnice znamená absolutní hodnotu reálného čísla, zatímco stejné symboly na pravé straně nerovnice označují velikost vektoru.

8.23 **Definice.** Nechť L je lineární prostor se skalárním součinem. *Vzdálenost vektoru* $\boldsymbol{x}$ *od vektoru* $\boldsymbol{y}$ definujeme jako $|\boldsymbol{y} - \boldsymbol{x}|$. Podle věty 8.19 je $|\boldsymbol{y} - \boldsymbol{x}| = |\boldsymbol{x} - \boldsymbol{y}|$, takže často mluvíme o *vzdálenosti dvou vektorů* $\boldsymbol{x}$ *a* $\boldsymbol{y}$ (bez závislosti na jejich pořadí).

8.24 **Věta.** (Trojúhelníková nerovnost). Pro velikosti vektorů platí

$$|\boldsymbol{x} + \boldsymbol{y}| \le |\boldsymbol{x}| + |\boldsymbol{y}|.$$

8.29 **Definice.** Nechť L je lineární prostor se skalárním součinem. Dva nenulové vektory $\boldsymbol{x} \in L$ a $\boldsymbol{y} \in L$ *jsou na sebe kolmé*, (značíme $\boldsymbol{x} \perp \boldsymbol{y}$), pokud je $\boldsymbol{x} \cdot \boldsymbol{y} = 0$.

8.31 **Definice.** Nechť $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ je báze lineárního prostoru se skalárním součinem. Bázi B nazýváme *ortogonální*, pokud $\boldsymbol{b}_i \perp \boldsymbol{b}_j$ $\forall i \in \{1, 2, \ldots, n\}$, $\forall j \in \{1, 2, \ldots, n\}$, $i \neq j$.
Bázi B nazýváme *ortonormální*, pokud je ortogonální, a navíc $|\boldsymbol{b}_i| = 1$, $\forall i \in \{1, 2, \ldots, n\}$.

8.32 **Věta.** Báze $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ je ortonormální právě tehdy, když

$$\boldsymbol{b}_i \cdot \boldsymbol{b}_j = \begin{cases} 0 \text{ pro } i \neq j, \\ 1 \text{ pro } i = j. \end{cases}$$

8.33 **Věta.** Nechť (B) je ortonormální uspořádaná báze lineárního prostoru L se skalárním součinem. Pak pro všechna $\boldsymbol{x} \in L$, $\boldsymbol{y} \in L$, $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)_{(B)}$, $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)_{(B)}$ lze skalární součin počítat ze souřadnic vektorů takto:

$$\boldsymbol{x} \cdot \boldsymbol{y} = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n.$$

8.35 **Věta.** Nechť $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ jsou nenulové vektory lineárního prostoru se skalárním součinem, které jsou na sebe navzájem kolmé, tj. $\boldsymbol{x}_i \cdot \boldsymbol{x}_j = 0$ pro $i \neq j$ a $\boldsymbol{x}_i \cdot \boldsymbol{x}_i > 0$. Pak jsou tyto vektory lineárně nezávislé.

8.36 **Věta.** Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je ortonormální báze lineárního prostoru se skalárním součinem. Pak pro souřadnice libovolného vektoru $\boldsymbol{x}$ platí

$$\boldsymbol{x} = (\boldsymbol{x}\cdot\boldsymbol{b}_1,\ \boldsymbol{x}\cdot\boldsymbol{b}_2,\ \ldots,\ \boldsymbol{x}\cdot\boldsymbol{b}_n)_{(B)}.$$

8.38 **Věta.** Nechť $(B) = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ je ortonormální báze lineárního prostoru se skalárním součinem a $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)_{(B)}$ je jeho libovolný vektor. Pak úhlel ϕ_i mezi vektorem $\boldsymbol{x}$ a vektorem $\boldsymbol{b}_i$ lze počítat podle vzorce

$$\cos\phi_i = \frac{x_i}{|\boldsymbol{x}|}.$$

8.41 **Věta.** (Schmidtův ortogonalizační proces). Nechť $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ je báze lineárního prostoru L se skalárním součinem. Pak existuje ortonormální báze $\{\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n\}$ taková, že

$$\langle \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k\rangle = \langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k\rangle, \qquad \forall k \in \{1, 2, \ldots, n\}$$

10.3 **Definice.** *Těleso* $\mathbf{Z}_2$ je dvoubodová množina $\{0, 1\}$, na které je definováno sčítání $+ : \mathbf{Z}_2 \times \mathbf{Z}_2 \to \mathbf{Z}_2$ a násobení $\cdot : \mathbf{Z}_2 \times \mathbf{Z}_2 \to \mathbf{Z}_2$ takto:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Tedy: $0 + 0 = 0$, $\quad 0 + 1 = 1 + 0 = 1$, $\quad 1 + 1 = 0$, $\quad 0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$, $1 \cdot 1 = 1$.

10.13 **Definice.** Nechť A je konečná množina (tzv. *abeceda*). Pak *slovo* je libovolná konečná posloupnost prvků z A.
Kódování v obecném smyslu zahrnuje (1) algoritmus, kterým informace převádíme do posloupnosti slov (tzv. *kodér*) a (2) algoritmus, kterým zpětně z těchto slov získáváme původní informaci (*dekodér*).
Slova, která vytváří kodér, se nazývají *kódová slova*. Množina všech kódových slov se nazývá *kód*.
Je-li kód množinou slov stejné délky (každé kódové slovo má stejný počet znaků abecedy), mluvíme o tzv. *blokovém kódu*. Blokový kód *délky n* značí, že všechna kódová slova mají n znaků abecedy.

10.18 **Definice.** Nechť $A = \{0,1\}$. *Hammingova velikost slova* $\boldsymbol{u} \in A^n$ je počet jedniček v tomto slově a značíme ji $\|\boldsymbol{u}\|$. *Hammingova vzdálenost slov* $\boldsymbol{v} \in A^n$ *a* $\boldsymbol{w} \in A^n$ je počet bitů, ve kterých se tato dvě slova liší. Značíme ji $(\boldsymbol{v}, \boldsymbol{w})$.

10.25 **Definice.** Binární blokový kód K délky n je *lineární*, pokud K tvoří lineární podprostor lineárního prostoru $\mathbf{Z}_2^n$. Jestliže dimenzi tohoto podprostoru označíme k, pak mluvíme o *lineárním* (n,k) *kódu*.

10.26 **Věta.** Nejmenší Hammingova vzdálenost mezi slovy lineárního kódu K je rovna nejmenší Hammingově velikosti nenulového kódového slova.

10.32 **Definice.** *Generující matice lineárního kódu K* je po řádcích zapsaná báze tohoto kódu.
Kontrolní matice lineárního kódu K je taková matice $\mathbf{H}$ s lineárně nezávislými řádky, pro kterou platí: množina řešení homogenní soustavy $\mathbf{H}\boldsymbol{x} = \boldsymbol{o}$ je rovna kódu K.

10.33 **Věta.** Nechť $\mathbf{G}$ je generující matice a $\mathbf{H}$ kontrolní matice lineárního (n,k) kódu. Pak $\mathbf{G}$ má k řádků a $\mathbf{H}$ má $n-k$ řádků. Obě matice mají n sloupců. Jinými slovy generující matice má tolik řádků, kolik je v kódu informačních bitů, kontrolní matice má tolik řádků, kolik má kód kontrolních bitů a počet sloupců obou matic je roven počtu přenášených bitů v jednom slově.

10.37 **Věta.** Nechť $\mathbf{G}$ je generující a $\mathbf{H}$ je kontrolní matice lineárního (n,k) kódu. Pak $\mathbf{H}\cdot\mathbf{G}^T = \mathbf{O}_1$ a také $\mathbf{G}\cdot\mathbf{H}^T = \mathbf{O}_2$, kde $\mathbf{O}_1$ je nulová matice s $n-k$ řádky a k sloupci a $\mathbf{O}_2 = \mathbf{O}_1^T$.

10.40 **Definice.** Pokud existuje generující matice lineárního kódu ve tvaru $\mathbf{G} = (\mathbf{E}|\mathbf{C})$, kde $\mathbf{E}$ je jednotková matice, nazýváme takový kód *systematický*.

10.43 **Věta.** Kód je systematický právě tehdy když existuje kontrolní matice tohoto kódu tvaru $(\mathbf{C}^T|\mathbf{E}')$, kde $\mathbf{E}'$ je jednotková matice.

10.45 **Věta.** Nechť $\mathbf{G}$ je generující matice lineárního (n,k) kódu. Nechť dále $\mathcal{A} : \mathbf{Z}_2^k \to \mathbf{Z}_2^n$ je lineární zobrazení, které zobrazuje standardní bázi prostoru $\mathbf{Z}_2^k$ na řádky matice $\mathbf{G}$. Pak matice $\mathbf{G}^T$ je maticí lineárního zobrazení $\mathcal{A}$ vzhledem ke standardním bázím.

10.49 **Definice.** Nechť $\mathbf{H}$ je kontrolní matice lineárního kódu. *Syndrom* slova $\boldsymbol{w}$ je vektor $\boldsymbol{s}$, pro který platí $\boldsymbol{s}^T = \mathbf{H} \cdot \boldsymbol{w}^T$.
Nechť $\boldsymbol{v}$ je slovo vyslané kodérem a $\boldsymbol{w}$ je slovo přijaté dekodérem. Pak $\boldsymbol{e} = \boldsymbol{w} - \boldsymbol{v}$ je *chybové slovo*. Protože v $\mathbf{Z}_2^n$ je $-\boldsymbol{v} = \boldsymbol{v}$, chybové slovo lze počítat jako $\boldsymbol{w} + \boldsymbol{v}$.

10.51 **Věta.** Nechť K je lineární podprostor lineárního prostoru L a nechť $\boldsymbol{e}_1 \in L$, $\boldsymbol{e}_2 \in L$. Pak množiny $M_1 = \{\boldsymbol{e}_1 + \boldsymbol{v},\ \boldsymbol{v} \in K\}$, $M_2 = \{\boldsymbol{e}_2 + \boldsymbol{v},\ \boldsymbol{v} \in K\}$ jsou buď disjunktní nebo totožné.

10.52 **Věta.** Nechť $\boldsymbol{v}$ je kódové slovo a $\boldsymbol{e}$ je libovolné slovo. Pak slova $\boldsymbol{e}$ i $\boldsymbol{e}+\boldsymbol{v}$ mají stejný syndrom. Jinými slovy kódová slova modifikovaná stejnou chybou vytvářejí skupinu slov se společným syndromem.

10.56 **Věta.** Slovo s jednou jedničkou je kódové právě tehdy, když kontrolní matice obsahuje nulový sloupec. Dvě různá slova s jednou jedničkou mají společný syndrom právě tehdy, když kontrolní matice obsahuje aspoň dva stejné sloupce.