Kapitola 1

Počítání s maticemi

Definice 1.1 Matice typu $m \times n$ *je soubor* mn *čísel uspořádaný do obdélníkové tabulky o* m *řádcích a* n *sloupcích. Matice typu* $m \times m$ *se nazývá* čtvercová matice *řádu* m. *Matice typu* $m \times 1$ *se nazývá* sloupcový vektor *a matice typu* $1 \times n$ *se nazývá* řádkový vektor.

O číslech budeme předpokládat, že mají běžné vlastnosti, lze je sčítat a násobit, obě operace jsou komutativní a asociativní, spojuje je distributivita, existují nulový a jednotkový prvek, opačné a inverzní prvky. Takové vlastnosti mají například racionální, reálná nebo komplexní čísla, nebo také binární čísla.

Matice budeme značit velkými tučnými písmeny $\mathbf{A}, \mathbf{B}, \mathbf{C}$, atd. Prvky matic budeme značit malými písmeny. Tak například, napíšeme-li $\mathbf{A} = (a_{ij})$, znamená to, že v matici $\mathbf{A}$ je v i-tém řádku a j-tém sloupci prvek a_{ij}. Pokud budeme chtít v označení matice uvést i její typ, tak budeme psát $\mathbf{A}_{m\times n}$, případně $\mathbf{A} = (a_{ij})_{m\times n}$.

Definice 1.2 *Jsou-li* $\mathbf{A} = (a_{ij})$ *a* $\mathbf{B} = (b_{ij})$ *dvě matice stejného typu* $m \times n$, *pak definujeme* součet matic $\mathbf{A} + \mathbf{B}$ *jako matici* $(a_{ij} + b_{ij})$ *typu* $m \times n$.

Dále definujeme součin $b\mathbf{A}$ matice $\mathbf{A}$ *libovolného typu* $m \times n$ s číslem b *jako matici* $b\mathbf{A} = (ba_{ij})$ *typu* $m \times n$.

Ještě si zavedeme označení pro *nulovou matici* typu $m \times n$, tj. pro matici, jejíž všechny prvky jsou rovné číslu 0. Nulovou matici budeme značit $\mathbf{0}_{m\times n}$. A dále definujeme matici opačnou k matici $\mathbf{A} = (a_{ij})$ jako matici $-\mathbf{A} = (-a_{ij})$ typu $m \times n$.

Definice 1.3 *Řekneme, že dvě matice* $\mathbf{A} = (a_{ij}), \mathbf{B} = (b_{ij})$ *se rovnají, jestliže mají stejný typ* $m \times n$ *a platí* $a_{ij} = b_{ij}$ *pro každé* $i = 1, 2, \ldots, m$ *a každé* $j = 1, \ldots, n$,

Tvrzení 1.1 *Jsou-li* $\mathbf{A}, \mathbf{B}, \mathbf{C}$ *matice téhož typu* $m \times n$, *pak platí*

1. $\mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A}$,
2. $(\mathbf{A} + \mathbf{B}) + \mathbf{C} = \mathbf{A} + (\mathbf{B} + \mathbf{C})$,
3. $\mathbf{A} + \mathbf{0}_{m\times n} = \mathbf{A}$,
4. $\mathbf{A} + (-\mathbf{A}) = \mathbf{0}_{m\times n}$.

Důkaz. Prvek na místě (i, j) v matici $\mathbf{A} + \mathbf{B}$ se rovná $a_{ij} + b_{ij}$, na místě (i, j) v matici $\mathbf{B} + \mathbf{A}$ se rovná $b_{ij} + a_{ij}$. Sčítání čísel je komutativní, prvky na stejném místě v maticích $\mathbf{A} + \mathbf{B}$ a $\mathbf{B} + \mathbf{A}$ se rovnají, proto platí $\mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A}$.

Ostatní vlastnosti sčítání se dokáží zcela stejně. □

Tvrzení 1.2 *Pro libovolné dvě matice* $\mathbf{A}, \mathbf{B}$ *stejného typu* $m \times n$ *a libovolná dvě čísla* a, b *platí*

1. $(a + b)\mathbf{A} = a\mathbf{A} + b\mathbf{A}$,
2. $a(\mathbf{A} + \mathbf{B}) = a\mathbf{A} + a\mathbf{B}$,
3. $a(b\mathbf{A}) = (ab)\mathbf{A}$,
4. $1\mathbf{A} = \mathbf{A}$.

Důkaz. Postupujeme stejně jako v důkazu Tvrzení **??**. □

Následující definice je zobecněním vztahu mezi sloupcovým a řádkovým zápisem vektorů.

Definice 1.4 Transponovaná matice *k matici* $\mathbf{A}$ *typu* $m \times n$ *je matice* $\mathbf{A}^T = (b_{ij})$ *typu* $n \times m$, *kde* $b_{ij} = a_{ji}$ *pro libovolné indexy* $i = 1, 2, \ldots, n$ *a* $j = 1, 2, \ldots, m$.

Tvrzení 1.3 *Pro libovolné dvě matice* $\mathbf{A}, \mathbf{B}$ *stejného typu* $m \times n$ *a každé číslo* b *platí*

1. $(\mathbf{A} + \mathbf{B})^T = \mathbf{A}^T + \mathbf{B}^T$,

2. $(b\mathbf{A})^T = b\mathbf{A}^T$,

3. $(\mathbf{A}^T)^T = \mathbf{A}$.

Důkaz. Opět porovnáme prvky na stejných místech v maticích na obou stranách rovnosti.

Prvek na místě (i,j) v matici $(\mathbf{A}+\mathbf{B})^T$ se rovná prvku na místě (j,i) v matici $\mathbf{A}+\mathbf{B}$, tj. $a_{ji}+b_{ji}$. Prvek na místě (i,j) v matici $\mathbf{A}^T+\mathbf{B}^T$ se rovná součtu prvků na místě (i,j) v maticích $\mathbf{A}^T$ a $\mathbf{B}^T$, tj. $a_{ji}+b_{ji}$. □

Definice 1.5 *Je-li* $\mathbf{A}$ *matice typy* $m \times n$ *a* $\mathbf{B}$ *matice typu* $n \times p$*, pak definujeme* součin matic $\mathbf{AB} = (c_{ik})$ *jako matici typu* $m \times p$*, kde*

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

pro každé $i = 1, 2, \ldots, m$ *a každé* $k = 1, 2, \ldots, p$.

Dále definujeme jednotkovou matici $\mathbf{I}_n$ *řádu* n *jako čtvercovou matici* (a_{ij}) *řádu* n*, kde* $a_{ii} = 1$ *pro každé* i *a* $a_{ij} = 0$ *kdykoliv* $i \neq j$*, tj.*

$$\mathbf{I}_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Prvky jednotkové matice také označujeme pomocí Kroneckerova symbolu δ_{ij}. Ten se rovná 1 pokud $i = j$ a rovná se 0, pokud $i \neq j$.

Tvrzení 1.4 *Jsou-li* $\mathbf{A}, \mathbf{B}$ *matice typu* $m \times n$*,* $\mathbf{C}$ *matice typu* $n \times p$*,* $\mathbf{D}, \mathbf{E}$ *matice typu* $p \times q$ *a* a *číslo, pak platí*

1. $(\mathbf{BC})\mathbf{D} = \mathbf{B}(\mathbf{CD})$,

2. $(\mathbf{A}+\mathbf{B})\mathbf{C} = \mathbf{AC}+\mathbf{BC}$,

3. $\mathbf{C}(\mathbf{D}+\mathbf{E}) = \mathbf{CD}+\mathbf{CE}$,

4. $a(\mathbf{BC}) = (a\mathbf{B})\mathbf{C}$,

5. $(\mathbf{BC})^T = \mathbf{C}^T\mathbf{B}^T$,

6. $\mathbf{I}_m\mathbf{A} = \mathbf{A}\mathbf{I}_n = \mathbf{A}$.

Důkaz.
Ověřujeme, zda je operace proveditelná.
Porovnáváme typy matic na obou stranách rovnice.
Porovnáváme prvky na stejných místech.
1. $\mathbf{B}$ typu $m \times n$, $\mathbf{C}$ typu $n \times p$, $\mathbf{D}$ typu $p \times q$
$\mathbf{BC}$ typu $m \times p$, $\mathbf{CD}$ typu $n \times q$ - tedy součin je možný
$(\mathbf{BC})\mathbf{D}$ typu $m \times q$, $\mathbf{B}(\mathbf{CD})$ typu $m \times q$
- tedy na obou stranách rovnice jsou matice stejného typu
V matici $\mathbf{BC}$ je prvek na místě (i, k) roven

$$e_{ik} = \sum_{j=1}^{n} b_{ij} c_{jk}$$

V matici $(\mathbf{BC})\mathbf{D}$ je prvek na místě (i, l) roven

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

V matici $\mathbf{CD}$ je prvek na místě (j, l) roven

$$f_{jl} = \sum_{k=1}^{p} c_{jk} d_{kl}$$

V matici $\mathbf{B}(\mathbf{CD})$ je prvek na místě (i, l) roven

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

$\forall j, k, l : b_{ij}(c_{jk} d_{kl}) = (b_{ij} c_{jk}) d_{kl}$ - násobení je asociativní
Pozn.: prohazování sum - zajímá-li nás prvek na místě (i, l) a sumy jsou pro j, k, pak je můžeme prohodit
2. $\mathbf{A}$, $\mathbf{B}$ jsou typu $m \times n$, $\mathbf{C}$ je typu $n \times p$
$\mathbf{AC}$, $\mathbf{AC}$ jsou typu $m \times p$ - tedy operace jsou proveditelné
$(\mathbf{A} + \mathbf{B})\mathbf{C}$ je typu $m \times p$
$\mathbf{AC} + \mathbf{BC}$ je typu $m \times p$ - tedy na obou stranách rovnice jsou matice téhož typu
pvek na místě (i, j) v matici $\mathbf{A} + \mathbf{B}$ je roven $d_{ij} = a_{ij} + b_{ij}$

prvek na místě (i,k) v matici $(\mathbf{A}+\mathbf{B})\mathbf{C}$ je roven

$$\sum_{j=1}^{n} d_{ij}c_{jk} = \sum_{j=1}^{n}(a_{ij}+b_{ij})c_{jk} = \sum_{j=1}^{n} a_{ij}c_{jk} + \sum_{j=1}^{n} b_{ij}c_{jk}$$

prvek na místě(i,k) v matici $\mathbf{AC}$ je roven

$$\sum_{j=1}^{n} a_{ij}c_{jk}$$

prvek na místě (i,k) v matici $\mathbf{BC}$ je roven

$$\sum_{j=1}^{n} b_{ij}c_{jk}$$

prvek na místě (i,k) v matici $\mathbf{AC}+\mathbf{BC}$ je roven

$$\sum_{j=1}^{n} a_{ij}c_{jk} + \sum_{j=1}^{n} b_{ij}c_{jk}$$

3. analogicky jako 2
4. $\mathbf{B}$, $a\mathbf{B}$ jsou typu $m \times n$, $\mathbf{C}$ je typu $n \times p$ - tedy operace jsou proveditelné
$a(\mathbf{BC})$ je typu $m \times p$
$(a\mathbf{B})\mathbf{C}$ je typu $m \times p$ - tedy na obou stranách rovnice jou matice téhož typu
prvek na místě (i,k) v matici $\mathbf{BC}$ je roven

$$d_{ik} = \sum_{j=1}^{n} b_{ij}c_{jk}$$

prvek na místě (i,k) v matici $a(\mathbf{BC})$ je roven

$$ad_{ik} = a\sum_{j=1}^{n} b_{ij}c_{jk} = \sum_{j=1}^{n} ab_{ij}c_{jk}$$

prvek na místě (i,j) v matici $a\mathbf{B}$ je roven
$e_{ij} = ab_{ij}$
prvek na místě (i,k) v matici $(a\mathbf{B})\mathbf{C}$ je roven

$$\sum_{j=1}^{n} e_{ij}c_{jk} = \sum_{j=1}^{n} ab_{ij}c_{jk}$$

5. $\mathbf{B}$ je typu $m \times n$, $\mathbf{C}$ je typu $n \times p$
$\mathbf{C}^T$ je typu $p \times n$, $\mathbf{B}^T$ je typu $n \times m$ - tedy násobení je možné
$\mathbf{BC}$ je typu $m \times p$
$(\mathbf{BC})^T$ je typu $p \times m$
$\mathbf{C}^T\mathbf{B}^T$ je typu $p \times m$ - tedy na obou stranách rovnice jsou matice stejného typu
prvek na místě (i, k) v matici $\mathbf{BC}$ je roven

$$\sum_{j=1}^{n} b_{ij}c_{jk}$$

tj. prvek na místě (k, i) v matici $(\mathbf{BC})^T$
prvek na místě (k, j) v matici $\mathbf{C}^T$ je roven prvku na místě (j, k) v matici $\mathbf{C}$ tedy $d_{kj} = c_{jk}$
prvek na místě (j, i) v matici $\mathbf{B}^T$ je roven prvku na místě (i, j) v matici $\mathbf{B}$ tedy $e_{ji} = b_{ij}$
pvek na místě (k, i) v matici $\mathbf{C}^T\mathbf{B}^T$ je roven

$$\sum_{j=1}^{n} d_{kj}e_{ji} = \sum_{j=1}^{n} c_{jk}b_{ij} = \sum_{j=1}^{n} b_{ij}c_{jk}$$

6. $\mathbf{I}_m\mathbf{A} = \mathbf{A}$
$(m \times m)(m \times n)$
$\mathbf{I}_m = \delta_{ij}$
prvek na místě (i, k) v součinu $\mathbf{I}_m\mathbf{A}$ je roven

$$\sum_{j=1}^{m} \delta_{ij}a_{ik} = \delta_{ii}a_{ik} = a_{ik}$$

pro $\mathbf{AI}_n$ analogicky □

Pro čtvercovou matici $\mathbf{A}$ řádu n a kladné celé číslo k symbolem $\mathbf{A}^k$ označujeme součin k matic $\mathbf{A}$, tj. k-tou mocninu matice $\mathbf{A}$. Dále označíme $\mathbf{A}^0$ jednotkovou matici $\mathbf{I}_n$ téhož řádu n.

Příklad 1.1 Fibonacciova posloupnost

Příklad 1.2 Často používanou rovnost

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

můžeme snadno ověřit pomocí matice $\mathbf{A} = (a_{ij})$ typu $m \times n$.

V dvojité sumě nalevo vždy napřed sečteme prvky matice $\mathbf{A}$ po řádcích - suma $\sum_{j=1}^{n} a_{ij}$ je součet všech prvků matice $\mathbf{A}$, které leží v i-tém řádku. A poté sečteme tyto řádkové sumy. Na pravé straně napřed sečteme každý sloupec zvlášť a poté sečteme sloupcové sumy. V obou případech dostaneme součet všech prvků matice $\mathbf{A}$.

Definice 1.6 *Čtvercová matice* $\mathbf{A}$ *řádu* n *nazývá* regulární (invertovatelná), *jestliže existuje čtvercová matice* $\mathbf{B}$ *téhož řádu* n *taková, že platí* $\mathbf{BA} = \mathbf{AB} = \mathbf{I}_n$. *Matici* $\mathbf{B}$ *pak nazýváme* inverzní matice *k* $\mathbf{A}$ *a označujeme ji* $\mathbf{A}^{-1}$. *Čtvercová matice, která není regulární, se nazývá* singulární.

V případě regulární matice $\mathbf{A}$ můžeme definovat i záporné mocniny $\mathbf{A}^{-k}$ jako $(\mathbf{A}^{-1})^k$.

Tvrzení 1.5 *Inverzní matice k regulární matici je určena jednoznačně.*

Důkaz. Je-li $\mathbf{A}$ regulární matice řádu n a jsou-li $\mathbf{B}, \mathbf{C}$ inverzní matice k $\mathbf{A}$, pak platí

$$\mathbf{C} = \mathbf{I}_n\mathbf{C} = (\mathbf{BA})\mathbf{C} = \mathbf{B}(\mathbf{AC}) = \mathbf{BI}_n = \mathbf{B}.$$

□

Tvrzení 1.6 *Jsou-li* $\mathbf{A}, \mathbf{B}$ *regulární matice řádu* n *a* b *nenulové číslo, pak platí*

1. *součin* $\mathbf{AB}$ *je také regulární matice a* $(\mathbf{AB})^{-1} = \mathbf{B}^d$,
2. *matice* $b\mathbf{A}$ *je také regulární a* $(b\mathbf{A})^{-1} = b^{-1}\mathbf{A}^{-1}$,
3. *transponovaná matice* $\mathbf{A}^T$ *je také regulární matice a platí* $(\mathbf{A}^T)^{-1} = (\mathbf{A}^{-1})^T$,
4. *matice* $\mathbf{A}^{-1}$ *je také regulární a platí* $(\mathbf{A}^{-1})^{-1} = \mathbf{A}$.

Důkaz.
1. $(\mathbf{AB})(\mathbf{B}^{-1}\mathbf{A}^{-1}) = \mathbf{A}(\mathbf{B}\mathbf{B}^{-1})\mathbf{A}^{-1} = (\mathbf{A}\mathbf{I}_n)\mathbf{A}^{-1} = \mathbf{A}\mathbf{A}^{-1} = \mathbf{I}_n$
$(\mathbf{B}^{-1}\mathbf{A}^{-1})(\mathbf{AB}) = \mathbf{B}^{-1}(\mathbf{A}^{-1}\mathbf{A})\mathbf{B}^{-1} = (\mathbf{B}^{-1}\mathbf{I}_n)\mathbf{B}^{-1} = \mathbf{B}^{-1}\mathbf{B} = \mathbf{I}_n$
2. $(b\mathbf{A})(b^{-1}\mathbf{A}^{-1}) = (bb^{-1})(\mathbf{A}\mathbf{A}^{-1}) = 1 \cdot \mathbf{I}_n = \mathbf{I}_n$
$(b^{-1}\mathbf{A}^{-1})(b\mathbf{A}) = (b^{-1}b)(\mathbf{A}^{-1}\mathbf{A}) = 1 \cdot \mathbf{I}_n = \mathbf{I}_n$
3. $\mathbf{A}^T(\mathbf{A}^{-1})^T = (\mathbf{A}^{-1}\mathbf{A})^T = \mathbf{I}_n^T = \mathbf{I}_n$
$(\mathbf{A}^{-1})^T\mathbf{A}^T = (\mathbf{A}\mathbf{A}^{-1})^T = \mathbf{I}_n^T = \mathbf{I}_n$
4. $\mathbf{A}^{-1}\mathbf{A} = \mathbf{A}\mathbf{A}^{-1} = \mathbf{I}_n \rightarrow$ z definice regulární matice $\mathbf{A}^{-1}$ je regulární a inverzní k $(\mathbf{A}^{-1})^{-1}$ □

Definice 1.7 *Je-li* $\mathbf{A} = (a_{ij})$ *matice typu* $m \times n$*, pak pro každé* $i = 1, \ldots, m$ *nazýváme vektor* $(a_{i1}, a_{i2}, \ldots, a_{in})$ i*-tý* řádkový vektor matice $\mathbf{A}$ *a označujeme jej* $\mathbf{A}_{i*}$*. Podobně definujeme* j*-tý* sloupcový vektor matice $\mathbf{A}$ *jako vektor* $\mathbf{A}_{*j} = (a_{1j}, a_{2j}, \ldots, a_{mj})^T$ *pro* $j = 1, \ldots, m$*.*

Definice 1.8 *Jsou-li* $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_k$ *matice stejného typu a* $b_1, b_2, \ldots, b_k$ *čísla, pak součet*

$$b_1\mathbf{A}_1 + b_2\mathbf{A}_2 + \cdots + b_k\mathbf{A}_k$$

se nazývá lineární kombinace matic $\mathbf{A}_1, \ldots, \mathbf{A}_k$*. Čísla* $b_1, \ldots, b_k$ *nazýváme* koeficienty lineární kombinace*. Jsou-li matice* $\mathbf{A}_1, \ldots, \mathbf{A}_k$ *vektory, pak mluvíme o* lineární kombinaci vektorů*.*

Věta 1.7 *Je-li* $\mathbf{A} = (a_{ij})$ *matice typy* $m \times n$ *a* $\mathbf{B} = (b_{jk})$ *matice typu* $n \times p$*, pak*

1. *pro každé* $k = 1, \ldots, p$ *platí* $(\mathbf{AB})_{*k} = b_{1k}\mathbf{A}_{*1} + b_{2k}\mathbf{A}_{*2} + \cdots + b_{nk}\mathbf{A}_{*n} = \mathbf{AB}_{*k}$*,*
2. *pro každé* $i = 1, \ldots, m$ *platí* $(\mathbf{AB})_{i*} = a_{i1}\mathbf{B}_{1*} + a_{i2}\mathbf{B}_{2*} + \cdots + a_{im}\mathbf{B}_{m*} = \mathbf{A}_{i*}\mathbf{B}$*.*

Zkráceně můžeme předchozí větu formulovat tak, že k-tý sloupec součinu matic $\mathbf{AB}$ je lineární kombinací sloupců (levého činitele) $\mathbf{A}$ s koeficienty v k-tém sloupci matice $\mathbf{B}$ a i-tý řádek součinu $\mathbf{AB}$ se rovná lineární kombinaci řádků (pravého činitele) $\mathbf{B}$ s koeficienty v i-tém řádku matice $\mathbf{A}$.

Důkaz.
1. Prvek na místě (i, j) ve vektoru $(\mathbf{AB})_{*k}$ je roven prvku na místě (i, k) v součinu $\mathbf{AB}$, tj.

$$\sum_{j=1}^{n} a_{ij}b_{jk}$$

Prvek na místě (i,j) v

$$b_{1k}\mathbf{A}_{*1} + b_{2k}\mathbf{A}_{*2} + \cdots + b_{nk}\mathbf{A}_{*n} = \sum_{j=1}^{n} b_{jk}\mathbf{A}_{*j} = \sum_{j=1}^{n} b_{jk}a_{ij} = \sum_{j=1}^{n} a_{ij}b_{jk}$$

neboť prvek na místě (i,j) v $\mathbf{A}_{*j}$ se rovná a_{ij}
Prvek na místě (i,j) v $\mathbf{AB}_{*k}$ je roven

$$\sum_{j=1}^{n} a_{ij}\mathbf{B}_{*k} = \sum_{j=1}^{n} a_{ij}b_{jk}$$

neboť

$$\mathbf{B}_{*k} = \sum_{j=1}^{n} b_{jk}$$

2. analogicky jako 1 □

Definice 1.9 Soustavou m lineárních rovnic *o n neznámých rozumíme soustavu rovnic*

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

kde a_{ij} a b_i jsou známá čísla a x_j jsou neznámá čísla.

Matici $\mathbf{A} = a_{ij}$ nazýváme matice soustavy, *sloupcový vektor $\mathbf{b} = (b_1, b_2, \ldots, b_m)^T$ nazýváme* vektor pravých stran, *vektor $(x_1, x_2, \ldots, x_n)^T$ nazýváme* vektor neznámých *a matici $(\mathbf{A}|\mathbf{b})$ nazýváme* rozšířená matice soustavy. *Je-li vektor pravých stran $\mathbf{b}$ nulový, mluvíme o* homogenní soustavě lineárních rovnic.

Pomocí této terminologie můžeme soustavu lineárních rovnic z předchozí definice zapsat v maticovém tvaru

$$\mathbf{Ax} = \mathbf{b},$$

kde $\mathbf{A}$ je matice soustavy, $\mathbf{x}$ je vektor neznámých a $\mathbf{b}$ je vektor pravých stran.

Uvedeme ještě definice několika základních typů matic.

Definice 1.10 *Čtvercovou matici* $\mathbf{A} = a_{ij}$ *řádu* n *nazýváme*

1. symetrická, *platí-li* $\mathbf{A} = \mathbf{A}^T$, *tj.* $a_{ij} = a_{ji}$ *pro každé* $i, j = 1, \ldots, n$,
2. kososymetrická, *platí-li* $\mathbf{A} = -\mathbf{A}^T$, *tj.* $a_{ij} = -a_{ji}$ *pro každé* $i, j = 1, \ldots, n$,
3. horní trojúhelníková, *platí-li* $a_{ij} = 0$ *kdykoliv* $i > j$,
4. dolní trojúhelníková, *platí-li* $a_{ij} = 0$ *kdykoliv* $i < j$,
5. diagonální, *pokud* $a_{ij} = 0$ *kdykoliv* $i \neq j$.

U libovolné čtvercové matice řádu n *říkáme, že prvky* a_{ii} leží na hlavní diagonále *nebo že tvoří* hlavní diagonálu.

Úloha 1.1 Dokažte, že

1. součin symetrických matic je opět symetrická matice,
2. součin kososymetrických matic je symetrická matice,
3. součin horních trojúhelníkových matic je horní trojúhelníková matice,
4. součin dolních trojúhelníkových matic je dolní trojúhelníková matice,
5. součin diagonálních matic je diagonální matice,
6. pro každou čtercovou matici $\mathbf{A}$ je součet $\mathbf{A} + \mathbf{A}^T$ symetrická matice.

Rozklad matice do bloků

Někdy je výhodné nahlížet matici jako na rozdělenou do bloků. Rozdělíme-li matici $\mathbf{A}$ typu $m \times n$ podélně na prvních m_1 a zbylých $m_2 = m - m_1$ řádků a vertikálně na prvních n_1 sloupců a zbylých $n_2 = n - n_1$ sloupců, skládá se matice $\mathbf{A}$ ze čtyř bloků

$$\mathbf{A} = \left(\begin{array}{c|c} \overset{n_1}{\mathbf{A}_{11}} & \overset{n_2}{\mathbf{A}_{12}} \\ \hline \mathbf{A}_{21} & \mathbf{A}_{22} \end{array}\right) \begin{array}{l} m_1 \\ m_2 \end{array}$$

Každý blok $\mathbf{A}_{ij}$, $i, j = 1, 2$ je matice typu $m_i \times n_j$.

Je-li $\mathbf{B}$ matice typu $n \times p$ a rozdělíme-li ji do čtyř bloků následovně

$$\mathbf{B} = \left(\begin{array}{c|c} \mathbf{B}_{11} & \mathbf{B}_{12} \\ \hline \mathbf{B}_{21} & \mathbf{B}_{22} \end{array}\right) \begin{array}{l} p_1 \\ p_2 \end{array} \begin{array}{l} n_1 \\ n_2 \end{array},$$

kde $p_1 + p_2 = p$, pak lze snadno ověřit, že součin $\mathbf{AB}$ lze rozdělit do bloků následovně

$$\mathbf{AB} = \left(\begin{array}{c|c} \mathbf{C}_{11} & \mathbf{C}_{12} \\ \hline \mathbf{C}_{21} & \mathbf{C}_{22} \end{array}\right) \begin{array}{l} p_1 \\ p_2 \end{array} \begin{array}{l} m_1 \\ m_2 \end{array},$$

a pro každé $i, j = 1, 2$ platí

$$\mathbf{C}_{ij} = \mathbf{A}_{i1}\mathbf{B}_{1j} + \mathbf{A}_{i2}\mathbf{B}_{2j}.$$

Formulka pro součin matic rozdělených na čtyři bloky je speciálním případem podobné formule pro libovolné rozklady matic na bloky.

Definice 1.11 *Je-li* $\mathbf{A} = (a_{ij})$ *matice typu* $m \times n$, $m = m_1 + m_2 + \cdots + m_r$ *a* $n = n_1 + n_2 + \cdots + n_s$, *pak definujeme* rozklad matice $\mathbf{A}$ na bloky určený součty $m = m_1 + m_2 + \cdots + m_r$ *a* $n = n_1 + n_2 + \cdots + n_s$ *jako matici*

$$\mathbf{A} = \left(\begin{array}{c|c|c|c} \mathbf{A}_{11} & \mathbf{A}_{12} & \cdots & \mathbf{A}_{1s} \\ \hline \mathbf{A}_{21} & \mathbf{A}_{22} & \cdots & \mathbf{A}_{2s} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline \mathbf{A}_{r1} & \mathbf{A}_{r2} & \cdots & \mathbf{A}_{rs} \end{array}\right) \begin{array}{l} m_1 \\ m_2 \\ \vdots \\ m_r \end{array},$$

$\begin{array}{cccc} n_1 & n_2 & \cdots & n_s \end{array}$

kde matice $\mathbf{A}_{ij}$ *má typ* $m_i \times n_j$ *a na místě* (k, l) *v matici* $\mathbf{A}_{ij}$ *je prvek z místa* $(m_1 + \cdots + m_{i-1} + k, n_1 + \cdots + n_{j-1} + l)$ *v matici* $\mathbf{A}$. *Maticím* $\mathbf{A}_{ij}$ *říkáme* bloky rozkladu. *Píšeme také* $\mathbf{A} = (\mathbf{A}_{ij})$.

Následující tvrzení má jednoduchý důkaz, který pouze vyžaduje správně si napsat jednotlivé prvky ve všech maticích a jejich blocích.

Tvrzení 1.8 *Předpokládejme, že* $\mathbf{A}$ *je matice typu* $m \times n$, $\mathbf{B}$ *je matice typu* $n \times p$, $m = m_1 + m_2 + \cdots + m_r$, $n = n_1 + n_2 + \cdots + n_s$ *a* $p = p_1 + \cdots + p_t$. *Je-li* $\mathbf{A} = (\mathbf{A}_{ij})$ *rozklad matice* $\mathbf{A}$ *určený součty* $m = m_1 + m_2 + \cdots + m_r$ *a* $n = n_1 + n_2 + \cdots + n_s$, $\mathbf{B} = (\mathbf{B}_{jk})$ *je rozklad* $\mathbf{B}$ *určený součty* $n = n_1 + n_2 + \cdots + n_s$ *a* $p = p_1 + \cdots + p_t$ *a* $\mathbf{AB} = \mathbf{C}_{ik}$ *je rozklad součinu* $\mathbf{AB}$ *určený součty* $m = m_1 + m_2 + \cdots + m_r$ *a* $p = p_1 + \cdots + p_t$, *pak platí že pro každé* $i = 1, 2, \ldots, r$ *a pro každé* $k = 1, 2, \ldots, t$

$$\mathbf{C}_{ik} = \sum_{j=1}^{s} \mathbf{A}_{ij}\mathbf{B}_{jk}$$

Kapitola 2

Soustavy lineárních rovnic

Soustavy lineárních rovnic jsme zavedli v Definici **??**. Nejdříve si ukážeme dva případy, ve kterých lze soustavu řešit snadno. V případě, že matice soustavy je horní trojúhelníková s nenulovými prvky na hlavní diagonále, tj. tvaru

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1,n-1}x_{n-1} + a_{1n}x_n &= b_1 \\ a_{22}x_2 + \cdots + a_{2,n-1}x_{n-1} + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{n-1,n-1}x_{n-1} + a_{n-1,n}x_n &= b_{n-1}, \\ a_{n,n}x_n &= b_n, \end{aligned}$$

Takovou soustavu řešíme *zpětnou substitucí*, postupně počítáme jednotlivé neznámé $x_n, x_{n-1}, \ldots, x_1$ následovně

$$\begin{aligned} x_n &= a_{nn}^{-1}b_n, \\ x_{n-1} &= a_{n-1,n-1}^{n-1}(b_{n-1} - a_{n-1,n}x_n), \\ &\vdots \\ x_i &= a_{ii}^{-1}(b_i - a_{i,i+1}x_{i+1} - a_{i,i+2}x_{i+2} - \cdots - a_{in}x_n) \\ &\vdots \\ x_1 &= a_{11}^{-1}(b_1 - a_{12}x_2 - a_{13}x_3 - \cdots - a_{1n}x_n). \end{aligned}$$

Všimněme si, že v okamžiku, kdy spočítáme hodnotu x_i, už v dalších výpočtech nepotřebujeme hodnotu b_i. Můžeme proto využít místa v paměti,

kde byla zapsána hodnota b_i k zápisu hodnoty x_i. To vede k následujícímu algoritmu. Hodnotu vektoru neznámých $\mathbf{x}$ pak najdeme uloženou jako hodnotu $\mathbf{b}$. To vede k následujícímu algoritmu.

Algoritmus 2.1. Zpětná substituce

Vstup: Horní trojúhelníková matice $\mathbf{A}$ řádu n, vektor pravých stran $\mathbf{b}$ typu $n \times 1$,
Výstup: Řešení soustavy soustavy $\mathbf{Ax} = \mathbf{b}$,

for $i = n$ **to** 1
    if $a_{ii} = 0$ **set error**, **end**
    for $i = n$ **to** $i + 1$
        $b_i \leftarrow b_i - a_{ijb_j}$
    $b_i \leftarrow a_{ii}^{-1} b_i$
output b
end

Podobně snadno lze řešit soustavu s dolní trojúhelníkovou maticí pomocí *přímé substituce.*

Algoritmus 2.2. Přímá substituce

Vstup: Dolní trojúhelníková matice $\mathbf{A}$ řádu n, vektor pravých stran $\mathbf{b}$ typu $n \times 1$,
Výstup: Řešení soustavy soustavy $\mathbf{Ax} = \mathbf{b}$,

for $i = 1$ **to** n
    if $a_{ii} = 0$ **set error**, **end**
    for $i = 1$ **to** $i - 1$
        $b_i \leftarrow b_i - a_{ijb_j}$
    $b_i \leftarrow a_{ii}^{-1} b_i$
output b
end

V případě soustavy rovnic $\mathbf{Ax} = \mathbf{b}$ s obecnou maticí $\mathbf{A}$ provádíme ekvivalentní úpravy tak, abychom dostali matici, která se "co nejvíce" blíží horní trojúhelníkové matici. Nejddříve definujeme, co je to ekvivalentní úprava.

Definice 2.1 Ekvivalentní úprava *soustavy rovnic je taková úprava, po které se množina všech řešení* původní soustavy *rovná množině všech řešení* upravené soustavy.

Ukazuje se, že při řešení soustav lineárních rovnic vystačíme s úpravami tří typů.

1. *Ekvivaletní úprava prvního typu* je prohození dvou rovnic soustavy,
2. *ekvivalentní úprava druhého typu* je vynásobení nějaké rovnice soustavy *nenulovým* číslem a,
3. *ekvivalentní úprava třetího typu* je přičtení a-násobku nějaké rovnice k nějaké *jiné rovnici.*

Všimněmě si, že efekt kterékoliv z těchto úprav můžeme odstranit použitím nějaké jiné ekvivalentní úpravy, tj. z upravené soustavy můžeme znovu dostat původní soustavu použitím nějaké jiné ekvivalentní úpravy. V případě první ekvivaletní úpravy prohodíme ještě jednou prohozené řádky, v případě druhé úpravy vynásobíme stejnou rovnici číslem a^{-1}, a v případě třetí úpravy přičteme ke stejné rovnici $(-a)$-násobek téže rovnice, kterou jsme přičítali. Tohoto pozorování využijeme při důkazu následujícího tvrzení.

Tvrzení 2.1 *Úpravy všech tří typů jsou ekvivalentní úpravy soustavy lineárních rovnic.*

Důkaz.
1. jakékoli řešení $x_1, \ldots, x_n$ původní soustavy je i řešením upravené soustavy
2. Je-li $x_1, \ldots, x_n$ řešením původní soustavy, platí:
$a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n = b_k \forall k = 1, \ldots, n,$
Pro $k = i$ odtud plyne:
$aa_{i1}x_1 + aa_{i2}x_2 + \cdots + aa_{in}x_n = ab_i$
Tedy opět je $x_1, \ldots, x_n$ řešením každé rovnice nové soustavy
3. Každé $x_1, \ldots, x_n$ řešení původní soustavy je řešením
$(a_{i1} + aa_{j1})x_1 + \cdots + (a_{in} + aa_{jn})x_n = b_i + ab_j$
a je také ešením všech ostatních rovnic nové soustavy
Tedy každé řešení původní soustavy je řešením upravené soustavy, kterou jsme dostali z původní soustavy nějakou ekvivalentní úpravou
Rovněž každé řešení upravené soustavy je i řešením původní soustavy, protože každé ekvivalentní úprava je vratná □

Třem uvedeným typům úprav soustavy rovnic odpovídají elementární řádkové úpravy matice.

Definice 2.2 Elementární řádkovou úpravou matice $\mathbf{A}$ *typu* $m \times n$ *rozumíme kteroukoliv z následujících tří úprav*

1. *úprava prvního typu prohazuje k-tý a l-tý řádek matice pro $k \neq l$,*
2. *úprava druhého typu je vynásobení k-tého řádku číslem a pro $i = 1, 2, \ldots, m$,*
3. *úprava třetího typu je přičtení a-násobku l-tého řádku ke k-tému řádku pro $k \neq l$.*

V upravené matici je každý řádek lineární kombinací řádků původní matice. Podle Věty**??**.1 lze takovou úpravu matice získat tak, že ji vynásobíme zleva vhodnou čtvercovou maticí řádu m.

Definice 2.3 *Čtvercovou matici $\mathbf{E}$ řádu m nazýváme elementární matice, je-li jednoho ze tří následujících typů:*

1. *matice prvního typu $\mathbf{E}_{kl} = (a_{ij})$, kde $a_{kl} = a_{lk} = 1$, $a_{ii} = 1$ pro každé $i \neq k, l$ a všechny ostatní prvky jsou rovné nule, tj.*

$$\mathbf{E}_{kl} = \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}.$$

2. *matice druhého typu $\mathbf{E}_k(a) = (a_{ij})$, kde $\mathbf{E}_k(a)$ je diagonální matice s prvky $a_{kk} = a$, $a_{ii} = 1$ pro $i \neq k$, a $a_{ij} = 0$ pro $i \neq j$,*
3. *matice třetího typu $E_{kl}(a) = (a_{ij})$, kde $a_{ii} = 1$ pro každé $i = 1, \ldots, m$, $a_{kl} = a$, a všechny ostatní prvky matice $E_{kl}(a)$ jsou nulové.*

Tvrzení 2.2 *Elementární řádkovou úpravu matice $\mathbf{A}$ dostaneme tak, že ji vynásobíme zleva příslušnou elementární maticí.*

Definice 2.4 *Řekneme, že matice $\mathbf{B} = (b_{ij})$ typu $m \times n$ je v* řádkově odstupňovaném tvaru, *jestliže existuje nezáporné celé číslo $k \leq m$ a čísla $1 \leq j_1 < j_2 < \cdots < j_m \leq n$ taková, že platí*

1. *pro každé $i > k$ platí $\mathbf{B}_{i*} = \mathbf{0}$, tj. všechny tyto řádky jsou nulové,*

2. *pro každé* $i = 1, 2, \ldots, k$ *platí* $b_{ij_i} \neq 0$,

3. *pro každé* $i = 1, 2, \ldots, k$ *a každé* $j < j_i$ *platí* $b_{ij} = 0$.

Sloupce B_{*j_i} *nazýváme* bázové sloupce *matice* $\mathbf{B}$.

Algoritmus 2.3. Gaussova eliminace

Vstup: Matice $\mathbf{A}$ typu $m \times n$.
Výstup: Matice $\mathbf{C}$ typu $m \times n$ v řádkově odstupňovaném tvaru.
1. Najde (zleva) první nenulový sloupec

- Pokud žádný nenajde $\rightarrow \mathbf{A} = \mathbf{0}_{m\times n}$ a ta je v řádkově odstupňovaném tvaru.
- Pokud $\mathbf{A} \neq \mathbf{0}_{m\times n}$, ozačí j_1 nejmenší index nenulového sloupce v $\mathbf{A}$.

2. Pokud $a_{ij_i} \neq 0$, pak prohodí 1. a i-tý řádek.
3. Je teba vynulovat prvky pod a_x (nenulový člen v prvním řádku).

- Pokud $a_{1j_1} \neq 0$, $\forall i \geq 2$ přičteme k i-tému řádku $a_{ij_i} - \frac{a_{ij_1}}{a_{1j_1}}$ násobek prvního řádku.

4. Pak použijeme algoritmus znovu pro matici $\mathbf{B}$ tvoenou řádky $2, \ldots, n$ a sloupci $j_1 + 1, \ldots, n$ matice $\mathbf{A}$

$$\left(\begin{array}{c|cc} a_x & \ldots & a_{1n} \\ \hline 0 & \multirow{2}{*}{$\mathbf{B}$} & \vdots \\ 0 & & \ddots \end{array}\right)$$

Věta 2.3 *Gaussova eliminace převede libovolnou matici* $\mathbf{A}$ *typu* $m \times n$ *do řádkově odstupňovaného tvaru.*

Důkaz. Indukcí podle m
1. je-li $m = 1$, pak $\begin{pmatrix} 0 & 0 & a & \cdots & \cdots & \cdots \end{pmatrix}$ je v řádkově odstupňovaném tvaru
2. je-li $m > 1$, předpokládáme, že Gaussova eliminace převede do řádkově odstupňovaného tvaru libovolnou matici, která má $m - 1$ řádků
3. pomocí kroků 1, 2, 3 (Algoritmus 2.3) najdeme j_1, dále použijeme indukční předpoklad. □

Věta 2.4 *Soustava m lineárních rovnic o n neznámých* $\mathbf{Ax} = \mathbf{b}$ *je řešitelná právě když Gaussova eliminace převede rozšířenou matici soustavy* $(\mathbf{A}|\mathbf{b})$ *do matice* $(\mathbf{B}|\mathbf{c})$ *v řádkově odstupňovaném tvaru, ve které sloupec pravých stran* $\mathbf{c}$ *není bázový sloupec.*

Důkaz. Je-li sloupec pravých stran $\mathbf{c}$ bázový, existuje k (poslední nenulový řádek) tak, že $c_k \neq 0 \wedge b_{kj} = 0 \ \forall j = 1, \ldots, n$
Tj. po elementárních úpravách původní soustavy dostaneme rovnici
$b_{k_1} x_1 + \cdots + b_{k_n} x_n = c_k$
$b_{k_1} x_1 + \cdots + b_{k_n} x_n = 0$
$c_k \neq 0$
Tato rovnice je nesplnitelná, tedy ani původní soustava není řešitelná.
Nechť sloupec pravých stran $\mathbf{c}$ není bázový.
Nechť k je počet nenulových sloupců, $j_1, \ldots, j_k$ splňují podmínky z definice řádkově odstupňovaného tvaru.
Máme matici $(\mathbf{E}|\mathbf{c})$, zvolme libovolně bodnoty $x_j \ \forall j \neq j_1, \ldots, j_k$ ($\rightarrow$ vystupují jako parametry)
$\mathbf{E} = (b_{ij})$, $\mathbf{c} = \begin{pmatrix} c_1 & \cdots & c_m \end{pmatrix}^T$
$\mathbf{Ex} = \mathbf{c} \Leftrightarrow \mathbf{Ax} = \mathbf{b}$ (s původní soustavou)
jdeme odspodu:

$$b_{1j_1} x_{j_1} + \cdots + b_{1j_{k-1}} x_{j_{k-1}} + b_{1j_k} x_{j_k} = c_1 - \sum_{j \neq j_1, \ldots, j_k} b_{1j} x_j$$

$$\vdots$$

$$b_{k-1j_{k-1}} x_{j_{k-1}} + b_{k-1j_k} x_{j_k} = c_{k-1} - \sum_{\substack{j > j_{k-1} \\ j \neq j_k}} b_{k-1j} x_j$$

$$b_{kj_k} x_{j_k} = c_k - \sum_{j > j_k} b_{kj} x_j$$

u této soustavy známe pravé strany
je to soustava k rovnic o k neznámých $x_{j_1}, \ldots, x_{j_k}$
tyto prvky jsou nenulové (z definice řádkově odstupňovaného tvaru): $b_{1j_1}, b_{2j_2}, \ldots, b_{kj_k}$

Matice této soustavy je horní trojúhelníková s nenulovými prvky na hlavní diagonále - tato soustava má jednoznačné řešení, které získáme pomocí zpětné substituce □

Algoritmus 2.4. Obecná zpětná substituce

Efekt zaokrouhlovacích chyb

Špatně podmíněné soustavy

Tvrzení 2.5 *Všechny elementární matice jsou regulární.*

Důsledek 2.6 *Pro každou matici* $\mathbf{A}$ *typu* $m \times n$ *existuje regulární matice* $\mathbf{E}$ *taková, že matice* $\mathbf{EA}$ *je v řádkově odstupňovaném tvaru.*

Důkaz. Použijeme Gaussovu eliminaci na $\mathbf{A}$.
Z Věty **??** dostaneme matici v řádkově odstupňovaném tvaru.
Jednotlivé kroky Gaussovy eliminace jsou elementární řádkové úpravy a podle Tvrzení **??** existují elementární matice $\mathbf{E}_1, \ldots, \mathbf{E}_l$ tak,
že $\mathbf{E}_l \cdots \mathbf{E}_2\mathbf{E}_1\mathbf{A}$ je v řádkově odstupňovaném tvaru.
Podle Tvrzení **??** jsou všechny elementární matice regulární.
Podle Tvrzení **??**.1 je regulární také jejich součin $\mathbf{E}_l \cdots \mathbf{E}_2\mathbf{E}_1$. □

Věta 2.7 *Pro čtvercovou matici* $\mathbf{A}$ *řádu* n *jsou následující podmínky ekvivalentní:*

1. *matice* $\mathbf{A}$ *je regulární,*
2. *soustava* $\mathbf{Ax} = \mathbf{b}$ *má právě jedno řešení pro každou pravou stranu* $\mathbf{b}$,
3. *homogenní soustava* $\mathbf{Ax} = \mathbf{0}$ *má právě jedno řešení,*
4. *Gaussova eliminace použitá na matici* $\mathbf{A}$ *vede k matici v řádkově odstupňovaném tvaru* $\mathbf{B} = (b_{ij})$, *která má všechny řádky nenulové,*
5. *matici* $\mathbf{A}$ *lze převést pomocí elementárních řádkových úprav do jednotkové matice* $\mathbf{I}_n$,
6. *existuje regulární matice* $\mathbf{E}$, *pro kterou platí* $\mathbf{EA} = \mathbf{I}_n$,
7. *existuje regulární matice* $\mathbf{C}$, *pro kterou platí* $\mathbf{AC} = \mathbf{I}_n$.

Důkaz.
$1 \to 2$
existuje matice $\mathbf{A}^{-1}$ - inverzní k $\mathbf{A}$
vynásobíme $\mathbf{Ax} = \mathbf{b}$ zleva $\mathbf{A}^{-1}$

$$\begin{aligned} \mathbf{A}^{-1}\mathbf{Ax} &= \mathbf{A}^{-1}\mathbf{b} \\ \mathbf{I}_n\mathbf{x} &= \mathbf{A}^{-1}\mathbf{b} \\ \mathbf{x} &= \mathbf{A}^{-1}\mathbf{b} \end{aligned}$$

je jednoznačně určené řešení
$2 \to 3$
speciální případ 2, kdy $\mathbf{b} = \mathbf{0}$
$\mathbf{x} = \mathbf{A}^{-1}\mathbf{0} = \mathbf{0}$
$3 \to 4$ (sporem)
Pokud by po převedení $\mathbf{A}$ do řádkově odstupňovaného tvaru na matici $\mathbf{B}$ pomocí Gaussovy eliminace byl poslední řádek nulový, existoval by sloupec v $\mathbf{B}$, který by nebyl bázový (neboť počet bázových sloupců je roven počtu nenulových řádků)
je-li jeho index j, můžeme x_j zvolit libovolně, např.: $x_j = 1$ a dopočítat řešení pomocí zpětné substituce; poté pro $x_j = 0 \to$ dostaneme alespoň 2 řešení $\to$ spor s 3
$4 \to 5$
Pomocí elementárních řádkových úprav dostaneme z $\mathbf{A}$ matici $\mathbf{B}$ v řádkově odstupňovaném tvaru a všechny sloupce jsou bázové.
Platí, že $k = n$ (k je počet nenulových řádků)
$1 \leq j_1 < j_2 < \ldots < j_n \leq n$
$1, 2, \ldots, n$ indexy řádků, tedy $j_i = i \ \forall i = 1, \ldots, n$
Matice $\mathbf{B}$ je horní trojúhelníková s nenulovými prvky na hlavní diagonále (tvoříme jednotkouvou matici pomocí elementárních řádkových úprav)
i-tý řádek vynásobíme $b_{ij}^{-1} \to$ získáme horní trojúhelníkovou matici, kde na hlavní diagonále jsou 1, tedy:
$\mathbf{C} = (c_{ij}), c_{ii} = 1 \ \forall i = 1, \ldots, n$
(postupně odečítáme násobky řádků pod - začneme od prvního řádku)
odečítáme c_{ji} násobek j-tého řádku pro $i > j$ pro $i = 1, \ldots, n$
$5 \to 6$
Existují elementární matice $\mathbf{E}_1, \ldots, \mathbf{E}_l$ tak, že $\mathbf{E}_l \cdots \mathbf{E}_2\mathbf{E}_1\mathbf{A} = \mathbf{I}_n$
Podle Tvrzení 2.5 je součin $\mathbf{E}_l \cdots \mathbf{E}_2\mathbf{E}_1$ regulární
$6 \to 7$
existuje $\mathbf{EA} = \mathbf{I}_n$, $\mathbf{E}$ je regulární, pak existuje $\mathbf{E}^{-1}$

$$(\mathbf{E}^{-1}\mathbf{E})\mathbf{A} = \mathbf{E}^{-1}\mathbf{I}_n$$

$$\begin{aligned} \mathbf{I}_n\mathbf{A} &= \mathbf{E}^{-1} \\ \mathbf{A} &= \mathbf{E}^{-1} \\ \mathbf{AE} &= \mathbf{E}^{-1}\mathbf{E} \\ \mathbf{AE} &= \mathbf{I}_n \end{aligned}$$

můžeme zvolit $\mathbf{C} = \mathbf{E}$
$7 \to 1$
$\mathbf{AC} = \mathbf{I}_n$, $\mathbf{C}$ je regulární

$$\begin{aligned} \mathbf{ACC}^{-1} &= \mathbf{C}^{-1} \\ \mathbf{A} &= \mathbf{C}^{-1} \\ \mathbf{CA} &= \mathbf{CC}^{-1} = \mathbf{I}_n \end{aligned}$$

□

Algoritmus 2.5. Výpočet inverzní matice

Tvrzení 2.8 *Nechť* $\mathbf{A}$ *je čtvercová matice řádu* n*. Potom pro čtvercovou matici* $\mathbf{B}$ *řádu* n *platí* $\mathbf{AB} = \mathbf{I}_n$ *právě když* $\mathbf{BA} = \mathbf{I}_n$*.*

Důkaz. $\to$ Dokážeme, že $\mathbf{A}$ je regulární tak, že dokážeme, že splňuje podmínku z Věty **??**, tedy, že $\mathbf{Ax} = \mathbf{0} \Rightarrow \mathbf{x} = \mathbf{0}$
Buď $\mathbf{x}$ (sloupcový vektor) takový, že $\mathbf{Ax} = \mathbf{0}$
Z $\mathbf{BA} = \mathbf{I}_n$ plyne $\mathbf{B}(\mathbf{Ax}) = \mathbf{I}_n\mathbf{x}$
$\mathbf{B0} = \mathbf{x}$
$\mathbf{0} = \mathbf{x}$
Podle Věty 2.7.3 je $\mathbf{A}$ regulární, tedy existuje $\mathbf{A}^{-1}$
Z $\mathbf{BA} = \mathbf{I}_n$ plyne
$\mathbf{B}(\mathbf{AA}^{-1}) = \mathbf{I}_n\mathbf{A}^{-1}$
$\mathbf{BI}_n = \mathbf{A}^{-1}$
$\mathbf{B} = \mathbf{A}^{-1}$
$\mathbf{AB} = \mathbf{I}_n$
$\leftarrow$ Dokážeme, že $\mathbf{B}$ je regulární tak, že dokážeme, že splňuje podmínku z Věty **??**, tedy, že $\mathbf{Bx} = \mathbf{0} \Rightarrow \mathbf{x} = \mathbf{0}$
Buď $\mathbf{x}$ (sloupcový vektor) takový, že $\mathbf{Bx} = \mathbf{0}$
Z $\mathbf{AB} = \mathbf{I}_n$ plyne $\mathbf{A}(\mathbf{Bx}) = \mathbf{I}_n\mathbf{x}$
$\mathbf{A0} = \mathbf{x}$

$\mathbf{0} = \mathbf{x}$
Podle Věty 2.7.3 je $\mathbf{B}$ regulární, tedy existuje $\mathbf{B}^{-1}$
Z $\mathbf{AB} = \mathbf{I}_n$ plyne
$\mathbf{A}(\mathbf{B}\mathbf{B}^{-1}) = \mathbf{I}_n\mathbf{B}^{-1}$
$\mathbf{A}\mathbf{I}_n = \mathbf{B}^{-1}$
$\mathbf{A} = \mathbf{B}^{-1}$
$\mathbf{B}\mathbf{A} = \mathbf{I}_n$ □

Tvrzení 2.9 *Buď* $\mathbf{B}$ *čtvercová matice řádu* n, $\mathbf{A}$ *regulární matice řádu* n *a* $a_1, a_2, \ldots, a_n$ *čísla. Potom platí*

$$a_1\mathbf{B}_{*1} + a_2\mathbf{B}_{*2} + \cdots + a_n\mathbf{B}_{*n} = \mathbf{0}$$

právě když

$$a_1(\mathbf{AB})_{*1} + a_2(\mathbf{AB})_{*2} + \cdots + a_n(\mathbf{AB})_{*n} = \mathbf{0}.$$

Důkaz. Pomocí Věty **??**: $(\mathbf{AB})_{*k} = b_{1k}\mathbf{A}_{*1} + b_{2k}\mathbf{A}_{*2} + \cdots + b_{nk}\mathbf{A}*n = \mathbf{AB}_{*k}$
$\rightarrow$ Je-li $a_1\mathbf{B}_{*1} + a_2\mathbf{B}_{*2} + \cdots + a_n\mathbf{B}_{*n} = \mathbf{0}$
$\mathbf{A}(a_1\mathbf{B}_{*1} + a_2\mathbf{B}_{*2} + \cdots + a_n\mathbf{B}_{*n}) = \mathbf{0}$
$\mathbf{A}a_1\mathbf{B}_{*1} + \mathbf{A}a_2\mathbf{B}_{*2} + \cdots + \mathbf{A}a_n\mathbf{B}_{*n} = \mathbf{0}$
$a_1(\mathbf{AB}_{*1}) + a_2(\mathbf{AB}_{*2}) + \cdots + a_n(\mathbf{AB}_{*n}) = \mathbf{0}$
$a_1(\mathbf{AB})_{*1} + a_2(\mathbf{AB})_{*2} + \cdots + a_n(\mathbf{AB})_{*n} = \mathbf{0}$

$\leftarrow$ Je-li $a_1(\mathbf{AB})_{*1} + a_2(\mathbf{AB})_{*2} + \cdots + a_n(\mathbf{AB})_{*n} = \mathbf{0}$
$a_1(\mathbf{AB}_{*1}) + a_2(\mathbf{AB}_{*2}) + \cdots + a_n(\mathbf{AB}_{*n}) = \mathbf{0}$
$\mathbf{A}a_1\mathbf{B}_{*1} + \mathbf{A}a_2\mathbf{B}_{*2} + \cdots + \mathbf{A}a_n\mathbf{B}_{*n} = \mathbf{0}$
$\mathbf{A}(a_1\mathbf{B}_{*1} + a_2\mathbf{B}_{*2} + \cdots + a_n\mathbf{B}_{*n}) = \mathbf{0}$
přenásobíme obě strany rovnice maticí $\mathbf{A}^{-1}$ ($\mathbf{A}$ je regulární)
$\mathbf{A}^{-1}\mathbf{A}(a_1\mathbf{B}_{*1} + a_2\mathbf{B}_{*2} + \cdots + a_n\mathbf{B}_{*n}) = \mathbf{A}^{-1}\mathbf{0}$
$\mathbf{I}_n(a_1\mathbf{B}_{*1} + a_2\mathbf{B}_{*2} + \cdots + a_n\mathbf{B}_{*n}) = \mathbf{0}$
$a_1\mathbf{B}_{*1} + a_2\mathbf{B}_{*2} + \cdots + a_n\mathbf{B}_{*n} = \mathbf{0}$
□

Příklad 2.1 Soustava rovnic pro výpočet proudů v elektrickém obvodu.

Všimněte si, že praktické úlohy často vedou přirozeně na soustavu rovnic s regulární maticí. Proudy v elektrickém obvodu nějak běhají, tedy řešení existuje, a navíc běhají jednoznačně, nelze si v nějakém okruhu proud zvolit

libovolně a dopočítat proudy ve zbylých okruzích. Soustava rovnic má tedy právě jedno řešení pro jakékoliv zdroje, tedy pro jakoukoliv pravou stranu.

Předchozí příklad ukazuje, že při řešení praktických problémů může nastat situace, kdy potřebujeme řešit soustavu $\mathbf{Ax} = \mathbf{c}$ poté, co jsme již vyřešili soustavu $\mathbf{Ax} = \mathbf{b}$. V tom případě je řešení pomocí Gaussovy eliminace značně neefektivní, při řešení soustavy $\mathbf{Ax} = \mathbf{c}$ bychom znovu museli převádět matici $\mathbf{A}$ do řádkově odstupňovaného tvaru, což jsme již dělali při řešení soustavy $\mathbf{Ax} = \mathbf{b}$. Existuje způsob, jak uchovat informace o průběhu Gaussovy eliminace ve formě speciálního rozkladu matice, tzv. LU-rozkladu, který usnadní řešení jiné soustavy se stejnou maticí soustavy a jinou pravou stranou.

Lemma 2.10 *Předpokládáme, že* $\mathbf{A}, \mathbf{B}$ *jsou dolní trojúhelníkové matice řádu* n *s jednotkami na hlavní diagonále. Potom platí*

1. *součin* $\mathbf{AB}$ *je také dolní trojúhelníkové matice s jednotkami na hlavní diagonále,*

2. *inverzní matice* $\mathbf{A}^{-1}$ *je také dolní trojúhelníková matice s jednotkami na hlavní diagonále.*

Důkaz. 1. $\mathbf{A} = (a_{ij}), a_{ij} = 0$ pro $i < j, a_{ii} = 1\ \forall i$
$\mathbf{B} = (b_{jk}), b_{jk} = 0$ pro $j < k, b_{jj} = 1\ \forall j$
$\mathbf{AB} = (c_{ik})$, chcem dokázat, že $c_{ik} = 0$ pro $i < k$

$$i < k \ldots c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}$$

$\forall j = 1, \ldots, n$ platí buď $j < k$, nebo $i > j$, tedy buď $b_{jk} = 0$, nebo $a_{ij} = 0$, pak $a_{ij} b_{jk} = 0\ \forall j = 1, \ldots, n$, tedy $\mathbf{AB}$ je dolní trojúhelníková.
Chceme dokázat, že $c_{ii} = 0\ \forall i$

$$c_{ii} = \sum_{j=1}^{n} a_{ij} b_{ji}$$

Je-li $j \neq i$ platí buď $i < j$, nebo $j < i$, tedy $a_{ij} b_{ji} = 0\ \forall j \neq i$
$c_{ii} = a_{ii} b_{ii} = 1\ \forall i$, tedy $\mathbf{AB}$ má jednoky na hlavní diaonále.
$\mathbf{A}^T$ ...je horní trojúhelníková matice s jednotkami na hlavní diagonále, tedy je v řádkově odstupňovaném tvaru.
Podle Věty **??** je regulární.
Podle Tvrzení **??** je i $\mathbf{A}$ regulární

Počítáme $\mathbf{A}^{-1}$ podle Algoritmu **??**, používáme pouze elementární řádkové úpravy 3. typu, používáme odpovídající elementární matice $\mathbf{E}_{kl}(a)$ - ty jsou dolní trojúhelníkové.
$a_{kl} = a, a_{ii} = 1$, ostatní prvky jsou 0.
Tedy existují dolní trojúhelníkové matice s jednotkami na hlavní diagonále $\mathbf{E}_1, \ldots, \mathbf{E}_p$ takové, že $\mathbf{E}_p \cdots \mathbf{E}_1 \mathbf{A} = \mathbf{I}_n$
$\mathbf{E}_p \cdots \mathbf{E}_1 = \mathbf{A}^{-1}$, tedy $\mathbf{A}^{-1}$ se rovná součinu dolních trojúhelníkových matic s jednotkami na hlavní diagonále, tedy je také dolní trojúhelníková s jednotkami na hlavní diagonále. □

Věta 2.11 *Předpokládáme, že* $\mathbf{A}$ *je regulární čtvercová matice řádu* n *taková, že při Gaussově eliminaci vystačíme pouze s elementárními řádkovými úpravami třetího typu. Potom existují jednoznačně určené čtvercové matice* $\mathbf{L}, \mathbf{U}$ *řádu* n *takové, že platí*

1. $\mathbf{L}$ *je dolní trojúhelníková matice s jednotkami na hlavní diagonále,*
2. $\mathbf{U}$ *je horní trojúhelníková matice s nenulovými prvky na hlavní diagonále,*
3. $\mathbf{A} = \mathbf{LU}$.

Důkaz. Dva důkazy existence, jeden pomocí Lemma **??**, druhý konstruktivnější pomocí multiplikátorů, který vede přímo k algoritmu pro kostrukci LU-rozkladu.
Důkaz č. 1: Na $\mathbf{A}$ provedeme Gaussovu eliminaci pomocí elementárních řádkových úprav 3. typu (odpovídají $\mathbf{E}_{kl}(a)$, která je dolní trojúhelníková s jednotkami na hlavní diagonále).
Existují matice $\mathbf{E}_1, \ldots, \mathbf{E}_p$ takové, že $\mathbf{E}_p \cdots \mathbf{E}_1 \mathbf{A} = \mathbf{U}$ v řádkově odstupňovaném tvaru (podle Věty **??** jsou všechny nenulové $\rightarrow$ tedy horní trojúhelníkové s nenulovými prvky na hlavní diagonále)
$\mathbf{E}_p \cdots \mathbf{E}_1 = \mathbf{E}$, $\mathbf{EA} = \mathbf{U}$
$\mathbf{E}$ je dolní trojúhelníková s jednotkami na hlavní diagonále, existuje $\mathbf{E}^{-1}$ dolní trojúhelníková s jednotkami na hlavní diagonále, tedy $\mathbf{A} = \mathbf{E}^{-1}\mathbf{U} = \mathbf{LU} \rightarrow \mathbf{E}^{-1} = \mathbf{L}$
Jednozačnost matic $\mathbf{L}, \mathbf{U}$:
Je-li $\mathbf{A} = \mathbf{L}_1\mathbf{U}_1$ a $\mathbf{A} = \mathbf{L}_2\mathbf{U}_2$
$\mathbf{L}_1, \mathbf{L}_2$ jsou dolní trojúhelníkové s jednotkami na hlavní diagonále.
$\mathbf{U}_1, \mathbf{U}_2$ jsou horní trojúhelníkové s nenulovými prvky na hlavní diagonále.

$$\mathbf{L}_1\mathbf{U}_1 \quad = \quad \mathbf{L}_2\mathbf{U}_2$$

$$\begin{aligned}\mathbf{L}_2^{-1}\mathbf{L}_1\mathbf{U}_1\mathbf{U}_1^{-1} &= \mathbf{L}_2^{-1}\mathbf{L}_2\mathbf{U}_2\mathbf{U}_1^{-1}\\ \mathbf{L}_2^{-1}\mathbf{L}_1 &= \mathbf{U}_2\mathbf{U}_1^{-1}\end{aligned}$$

na levé straně poslední rovnice je dolní trojúhelníková matice s jednotkami na hlavní diagonále, na pravé straně je horní trojúhelníková matice s nenulovými prvky na hlavní diagonále → jsou to tedy diagonální matice s jednotkami na hlavní diagonále, tedy:
$\mathbf{L}_2^{-1}\mathbf{L}_1 = \mathbf{I}_n \rightarrow \mathbf{L}_2 = \mathbf{L}_1$
$\mathbf{U}_2^{-1}\mathbf{U}_1 = \mathbf{I}_n \rightarrow \mathbf{U}_2 = \mathbf{U}_1$

Důkaz č. 2 (konstruktivní):

$$\mathbf{A} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$$

Protože stačí pouze elementární řádkové úpravy 3.typu, je $a_{11} \neq 0$, pak $m_{21} = a_{21}a_{11}^{-1}$, odečteme m_{21} násobek prvního řádku od druhého ...
→ obecně: $m_{i1} = a_{i1}a_{11}^{-1}$, odečteme m_{i1} násobek 1. řádku od i-tého
→ všechny prvky v 1. soupci vynulujeme pomocí matice $\mathbf{T}_1$ řádu n:

$$\mathbf{T}_1 = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 \\ -m_{21} & 1 & 0 & \dots & 0 \\ -m_{31} & 0 & \ddots & 0 & 0 \\ \vdots & 0 & \dots & 1 & 0 \\ -m_{n1} & 0 & \dots & 0 & 1 \end{pmatrix}$$

$$\mathbf{T}_1 = \mathbf{I}_n - c_i e_1^T$$

$$c_1 = \begin{pmatrix} 0 \\ m_{21} \\ \vdots \\ m_{n1} \end{pmatrix}, e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, c_1 e_1^T = \begin{pmatrix} 0 & \dots & \dots & 0 \\ m_{21} & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & 0 & \dots & 0 \end{pmatrix}$$

$$\mathbf{T}_1\mathbf{A} = \left(\begin{array}{c|ccc} a_{11} & a_{22} & \dots & a_{1n} \\ \hline 0 & a_{22}^{(2)} & \dots & a_{2n}^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2}^{(2)} & \dots & a_{nn}^{(2)} \end{array}\right)$$

Potom $a_{22}^{(2)} \neq 0$, $m_{i2} = a_{i2}^{(2)}(a_{22}^{(2)})^{-1}$

$$\mathbf{T}_2 = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & -m_{i2} & 1 & 0 & 0 \\ \vdots & \vdots & 0 & \ddots & 0 \\ 0 & -m_{n2} & 0 & \dots & 1 \end{pmatrix} = \mathbf{I}_n - c_2 e_2^T = \begin{pmatrix} 0 \\ 0 \\ m_{32} \\ \vdots \\ m_{n2} \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \end{pmatrix}$$

Gaussovu eliminaci bez prohazovaní řádků lze vyjádřit maticově:
$\mathbf{T}_{n-1} \cdots \mathbf{T}_1 \mathbf{A} = \mathbf{U}$, $\mathbf{T}_{n-1} \cdots \mathbf{T}_1$ je dolní trojúhelníková s jednotkami na hlavní diagonále

$$\mathbf{T}_k = \mathbf{I}_n - c_k e_k^T, c_k = \begin{pmatrix} 0 \\ 0 \\ m_{k+1} \\ \vdots \\ m_{ik} \end{pmatrix}$$

kde prvních k prvků je nulových,

$$e_k^T = \begin{pmatrix} 0 & \dots & \overset{k}{1} & 0 & \dots \end{pmatrix}$$

$\mathbf{A} = \mathbf{T}_1^{-1} \cdots \mathbf{T}_{n-1}^{-1} \mathbf{U}$, $\mathbf{T}_k^{-1} = \mathbf{I}_n + c_k e_k^T$

$$\begin{aligned} \mathbf{T}_k^{-1}\mathbf{T}_k = (\mathbf{I}_n + c_k e_k^T)(\mathbf{I}_n - c_k e_k^T) = \\ = \mathbf{I}_n + c_k e_k^T - c_k e_k^T - (c_k e_k^T)(c_k e_k^T) = \\ = \mathbf{I}_n + c_k (e_k^T c_k) e_k^T = \mathbf{I}_n \end{aligned}$$

$\mathbf{T}_1^{-1} \cdots \mathbf{T}_{n-1}^{-1} = (\mathbf{I}_n + c_1 e_1^T) \cdots (\mathbf{I}_n + c_{n-1} e_{n-1}^T) =$
$= \mathbf{I}_n + c_1 e_1^T + \cdots + c_{n-1} e_{n-1}^T + \mathbf{0} = \mathbf{L}$
Ostatní prvky jsou nulové, např.: $c_1(e_1^T c_2)e_2^T \rightarrow \forall i \leq j : c_i e_i^T c_j e_j^T = 0$
□

Definice 2.5 *Rozklad* $\mathbf{A} = \mathbf{LU}$ *popsaný v předchozí Větě* **??** *nazýváme LU-*rozklad matice $\mathbf{A}$.

Algoritmus 2.6. Výpočet *LU*-rozkladu

Analýzou konstruktivního důkazu předchozí věty a za použití následující definice můžeme předpoklad Věty**??** formulovat bez odkazu na průběh Gaussovy eliminace.

Definice 2.6 *Je-li* $\mathbf{A} = (a_{ij})$ *čtvercová matice řádu* n*, pak pro libovolné* $m = 1, 2, \ldots$ *definujeme* hlavní minor *matice* $\mathbf{A}$ *jako matici* $\mathbf{A}_m = (a_{ij})$ *řádu* m *tvořenou prvky ležícími v prvních* m *řádcích a prvních* m *sloupcích matice* $\mathbf{A}$*. Tj.*

$$\mathbf{A}_1 = (a_{11}), \mathbf{A}_2 = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \ldots, \mathbf{A}_m = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{pmatrix} \cdots$$

Věta 2.12 *LU-rozklad matice* $\mathbf{A}$ *řádu* n *existuje právě tehdy když je každý hlavní minor matice* $\mathbf{A}$ *regulární.*

Důkaz. $\rightarrow$ Pokud LU-rozklad existuje, $\mathbf{A} = \mathbf{LU}$
rozklad matice $\mathbf{L}$ do bloků, určený $n = k + (n - k)$:

$$\mathbf{L} = \begin{pmatrix} \mathbf{L}_{11} & \mathbf{L}_{12} = 0 \\ \mathbf{L}_{21} & \mathbf{L}_{22} \end{pmatrix}$$

rozklad matice $\mathbf{U}$ do bloků, určený $n = k + (n - k)$:

$$\mathbf{U} = \begin{pmatrix} \mathbf{U}_{11} & \mathbf{U}_{12} \\ \mathbf{U}_{21} = 0 & \mathbf{U}_{22} \end{pmatrix}$$

Tedy:

$$\mathbf{A} = \begin{pmatrix} \mathbf{L}_{11}\mathbf{U}_{11} & \ldots \\ \vdots & \ddots \end{pmatrix}$$

$\mathbf{A}_k = \mathbf{L}_{11}\mathbf{U}_{11}$ je hlavní minor ; součin $\mathbf{L}_{11}\mathbf{U}_{11}$ regulárních matic je také regulární
$\leftarrow$ Je-li každý hlavní minor matice $\mathbf{A}$ regulární, pak i matice $\mathbf{A}$ je regulární, pak podle Věty **??** existují jednoznačně určené matice $\mathbf{L}$, $\mathbf{U}$ takové, že $\mathbf{A} = \mathbf{LU}$ je LU-rozklad matice $\mathbf{A}$

□

Pokud známe *LU*-rozklad $\mathbf{A} = \mathbf{LU}$ matice $\mathbf{A}$, můžeme snadno vyřešit soustavu $\mathbf{Ax} = \mathbf{b}$. Přepíšeme si ji do tvaru $\mathbf{LUx} = \mathbf{b}$ a položíme $\mathbf{Ux} = \mathbf{y}$. Původní soustavu $\mathbf{Ax} = \mathbf{b}$ pak vyřešíme postupným řešením dvou soustav

$$\begin{aligned} \mathbf{Ly} &= \mathbf{b}, \\ \mathbf{Ux} &= \mathbf{y}, \end{aligned}$$

z nichž tu první vyřešíme pomocí přímé substituce (**U** je horní trojúhelníková matice s nenulovými prvky na hlavní diagonále) a druhou pomocí zpětné substituce.

Příklad 2.2 Počty operací pro Gaussovu eliminaci, výpočet inverzní matice, přímou a zpětnou substituci, LU-rozklad.

Kapitola 3

Tělesa

Definice 3.1 *Předpokládáme, že* $\mathbf{T}$ *je množina, na které jsou definované dvě operace – sčítání a násobení. Pokud tyto dvě operace splňují následující podmínky (axiomy), říkáme že množina* $\mathbf{T}$ *spolu s těmito operacemi tvoří* těleso. *Jsou to podmínky*

(A0) *součet* $a + b \in \mathbf{T}$ *pro libovolné* $a, b \in \mathbf{T}$,

(A1) *platí* $(a + b) + c = a + (b + c)$ *pro libovolné* $a, b, c \in \mathbf{T}$,

(A2) $a + b = b + a$ *pro libovolné dva prvky* $a, b \in \mathbf{T}$,

(A3) *existuje prvek* $0 \in \mathbf{T}$ *takový, že* $0 + a = a$ *pro každé* $a \in \mathbf{T}$,

(A4) *ke každému prvku* $a \in \mathbf{T}$ *existuje prvek* $-a \in \mathbf{T}$, *pro který platí, že* $(-a) + a = 0$.

To jsou všechny axiomy pro sčítání. Axiom (A0) říká, že množina $\mathbf{T}$ *je* uzavřená *na sčítání. Axiom (A1) je* asociativita *sčítání, axiom (A2) je* komutativita *sčítání. Axiomu (A3) říkáme existence* nulového prvku *nebo také* neutrálního prvku *vzhledem ke sčítání a axiomu (A4) pak existence* opačného prvku *vzhledem ke sčítání.*

Následují axiomy pro násobení:

(M0) *součin* $ab \in \mathbf{T}$ *pro libovolné* $a, b \in \mathbf{T}$,

(M1) *platí* $(ab)c = a(bc)$ *pro libovolné* $a, b, c \in \mathbf{T}$,

(M2) $ab = ba$ *pro libovolné dva prvky* $a, b \in \mathbf{T}$,

(M3) *existuje prvek* $1 \in \mathbf{T}$ *takový, že* $1a = a$ *pro každé* $a \in \mathbf{T}$,

(M4) *ke každému prvku* $0 \neq a \in \mathbf{T}$ *existuje prvek* $a^{-1} \in \mathbf{T}$, *pro který platí* $a^{-1}a = 1$.

Axiom (M0) vyjadřujeme slovy, že množina $\mathbf{T}$ *je* uzavřená *vzhledem k násobení, axiomy (M1) a (M2) říkají, že násobení je* asociativní *a* komutativní. *Axiom (M3) je existence* jednotkového prvku *nebo také* neutrálního prvku *vzhledem k násobení a axiom (M4) je axiom existence* inverzního prvku *vzhledem k násobení.*

Obě operace pak spojuje axiom distributivity

(D) *platí* $a(b + c) = ab + ac$ *pro libovolné tři prvky* $a, b, c \in \mathbf{T}$.

A nakonec axiom netriviality

(N) $0 \neq 1$.

Tvrzení 3.1 *V každém tělese* $\mathbf{T}$ *platí*

1. *nulový prvek je určený jednoznačně,*
2. *opačný prvek* $-a$ *je prvkem* $a \in \mathbf{T}$ *určený jednoznačně,*
3. *jednotkový prvek je určený jednoznačně,*
4. *prvek* a^{-1} *inverzní k prvku* $0 \neq a \in \mathbf{T}$, *je prvkem* a *určený jednoznačně,*
5. $0a = 0$ *pro libolný prvek* $a \in \mathbf{T}$,
6. *je-li* $ab = 0$, *pak buď* $a = 0$ *nebo* $b = 0$,
7. $(-1)a = -a$ *pro každý prvek* $a \in \mathbf{T}$,
8. *rovnice* $ax = b$, $a \neq 0$, *má vždy právě jedno řešení,*
9. *rovnice* $c + x = d$ *má vždy právě jedno řešení,*
10. *z rovnosti* $ab = ac$ *a předpokladu* $a \neq 0$, *vyplývá* $b = c$,
11. *z rovnosti* $a + b = a + c$ *plyne* $b = c$,
12. $(-a)(-b) = ab$ *pro každé dva prvky* $a, b \in \mathbf{T}$.

Všechny dosavadní poznatky o maticích a řešení soustav lineárních rovnic platí v libovolném tělese $\mathbf{T}$. Soustavou lineárních rovnic v tělese $\mathbf{T}$ rozumíme soustavu

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

kde jsou všechny koeficienty $a_{ij}, b_k \in \mathbf{T}$. Z axiomů tělesa a jejich bezprostředních důsledků pak vyplývá, že Gaussova eliminace a zpětná substituce vedou k řešením této soustavy, která všechna opět leží v tělese $\mathbf{T}$.

Podobně matice s prvky z tělesa $\mathbf{T}$ je matice $\mathbf{A} = (a_{ij})$, kde $a_{ij} \in \mathbf{T}$. Elementární řádkové úpravy matice s prvky z libovolného tělesa $\mathbf{T}$ můžeme provádět beze změny. Je-li $\mathbf{A}$ regulární matice, pak pomocí elementárních řádkových úprav použitých na jednotkovou matici dostaneme inverzní matici $\mathbf{A}^{-1}$, která má také všechny prvky z tělesa $\mathbf{T}$. Podobně zůstávají v platnosti i všechny ostatní vlastnosti matic. Stačí pouze vždy na začátku říct, v jakém tělese leží prvky matic, se kterými počítáme. Tak například faktory $\mathbf{L}, \mathbf{U}$ v LU-rozkladu matice $\mathbf{A}$, která má prvky z tělesa $\mathbf{T}$, jsou oba také matice s prvky z tělesa $\mathbf{T}$.

Příklad 3.1 Příklady těles $\mathbf{Q}, \mathbf{R}, \mathbf{C}$, netěleso $\mathbf{Z}$, pro které nicméně řada poznatků také platí, jsou to všechny, které nezávisí na existenci inverzního prvku.

Příklad 3.2 Dvouprvková množina $\{0, 1\}$ spolu s operacemi sčítání

$$0 + 0 = 1 + 1 = 0, \quad 0 + 1 = 1 + 0 = 1,$$

a násobení

$$1 \cdot 1 = 1, \quad 0 \cdot 1 = 1 \cdot 0 = 0 \cdot 0 = 0$$

je také těleso. Je to vlastně počítání *modulo* 2. Výsledek operace získáme tak, že uděláme napřed obvyklý součet dvou čísel a za výsledek pak vezmeme zbytek při dělení obvyklého součtu číslem 2. Podobně pro součin. Platnost všech axiomů tělesa můžeme pak ověřit přímo. Toto těleso budeme označovat $\mathbf{Z}_2$.

Příklad 3.3 Jiné konečné těleso dostaneme, když čísla $\{0,1,2\}$ sčítáme a násobíme *modulo* 3. Operace sčítání je potom

$$0+0=1+2=2+1=0,\ 0+1=1+0=2+2=1,\ 0+2=2+0=1+1=2,$$

a operace násobení je

$$0\cdot 0=0\cdot 1=1\cdot 0=0\cdot 2=2\cdot 0=0,\ 1\cdot 1=2\cdot 2=1,\ 1\cdot 2=2\cdot 1=2.$$

Můžete si sami ověřit, že množina $\{0,1,2\}$ s takto definovanými operacemi je těleso. V případě asociativity obou operací a distributivity je třeba vždy ověřit 27 rovností.

Příklad 3.4 Množina $\{0,1,2,3\}$ spolu s operacemi sčítání a násobení *modulo* 4 **není** těleso. Platí v ní totiž $2\cdot 2=0$ a přitom $2\neq 0$. To se v žádném tělese nemůže stát podle Tvrzení **??**.6.

Příklad 3.5 Čtyřprvkové těleso ale existuje. Nejlépe je počítat s polynomy $\mathbf{GF}(4)=\{0,1,x,x+1\}$ jedné proměnné s koeficienty $0,1$. Koeficienty považujeme za prvky tělesa $\mathbf{Z}_2$. Tyto polynomy pak můžeme sčítat a násobit obvyklým způsobem. Množina $\mathbf{GF}(4)$ je uzavřená na sčítání polynomů, není ale uzavřená na jejich násobení, neboť $(x+1)(x+1)=x^2+(1+1)x+1=x^2+1$. Operaci násobení proto definujeme *modulo* polynom x^2+x+1. To znamená, že obvyklý součin dvou polynomů vydělíme se zbytkem polynomem x^2+x+1 a jako výsledek součinu vezmeme tento zbytek. Potom platí např.

$$x(x+1)=(x+1)x=1 \quad \text{a} \quad (x+1)(x+1)=x.$$

Zkuste si sami ověřit axiomy tělesa a dokázat, že množina $\mathbf{GF}(4)$ je skutečně těleso.

Příklad 3.6 Množina $\mathbf{Z}_n=\{0,1,2,\ldots,n-1\}$ pro $n\geq 2$ spolu s operacemi sčítání a násobení *modulo* n je těleso právě když je n prvočíslo. Toto tvrzení si nebudeme dokazovat. Pokud někdo zná Euklidův algoritmus, tak to zvládne sám. Jediný problém spočívá v důkazu existence inverzního prvku k libovolnému číslu $0\neq x<n$, pokud je n prvočíslo. Pokud n není prvočíslo, tak $\mathbf{Z}_n$ není tělesem ze stejného důvodu, kvůli kterému není $\mathbf{Z}_4$ těleso.

Příklad 3.7 Pro každé prvočíslo p a každý exponent $n \geq 1$ existuje právě jedno těleso, které má p^n prvků a žádná jiná tělesa s konečným počtem prvků neexistují. Žádné šestiprvkové těleso tedy neeistuje. Tělesa s počtem prvků p^n pro $n \geq 2$ se konstruují podobně, jako jsme sestrojili čtyřprvkové těleso v Příkladu **??**. Vezmeme všechny polynomy (včetně konstantních) stupně menšího než n s koeficienty v tělese $\mathbf{Z}_p$. Těch je celkem p^n. Na této množině sčítáme obvyklým způsobem a násobíme *modulo* **vhodný** polynom stupně n.

Vidíme, že tělesa mohou být značně odlišná. jejich vlastnosti hodně závisí na následujícím číselném parametru.

Definice 3.2 *Existuje-li kladné celé číslo n takové, že v tělese* $\mathbf{T}$ *platí*

$$\underbrace{1+1+\cdots+1}_{n} = 0,$$

pak nejmenší takové kladné číslo nazýváme charakteristika *tělesa* $\mathbf{T}$.

Pokud žádné takové kladné celé číslo n neexistuje, tak říkáme, že těleso $\mathbf{T}$ *má* charakteristiku 0.

Věta 3.2 *Charakteristika každého tělesa je buď 0 nebo prvočíslo.*

Důkaz. Jestliže charakteristika tělesa $\mathbf{T}$ není rovná 0, pak existuje nějaké kladné celé číslo $n \geq 2$, pro které platí

$$\underbrace{1+1+\cdots+1}_{n} = 0.$$

Jestliže je n složené číslo, platí $n = kl$ pro nějaká kladná celá čísla $k, l < n$. V důsledku axiomu distributivity (D) platí

$$(\underbrace{1+1+\cdots+1}_{k})(\underbrace{1+1+\cdots+1}_{l}) = \underbrace{1+1+\cdots+1}_{n} = 0.$$

Podle Tvrzení **??**.6 může být součin dvou prvků v tělese rovný 0 pouze pokud je aspoň jeden z činitelů rovný 0. Proto je buď

$$\underbrace{1+1+\cdots+1}_{k} = 0$$

nebo

$$\underbrace{1+1+\cdots+1}_{l} = 0.$$

V každém případě nemůže být složené číslo $n \geq 2$ nejmenším kladným celým číslem, pro které platí

$$\underbrace{1 + 1 + \cdots + 1}_{n} = 0.$$

Protože je $1 \neq 0$ podle axiomu netriviality (N), musí být nejmenší takové číslo prvočíslo. □

Úloha 3.1 Zjistěte charakteristiky těles $\mathbf{Z}_2$, $\mathbf{Z}_3$, $\mathbf{Q}$, $\mathbf{R}$ a $\mathbf{C}$. Jakou má charakteristiku konečné těleso, které má p^n prvků?

Kapitola 4

Aritmetické vektorové prostory

V této kapitole se budeme více zabývat sloupcovými a řádkovými vektory matic s prvky z libovolného tělesa. Napřed ale drobná úprava terminologie a značení.

Definice 4.1 Aritmetický vektor *dimenze n nad tělesem* $\mathbf{T}$ *je sloupcový vektor typu* $n \times 1$ *s prvky z tělesa* $\mathbf{T}$.

Aritmetické vektory budeme psát malými tučnými písmeny.

Definice 4.2 *Je-li* $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$ *aritmetický vektor dimenze n nad tělesem* $\mathbf{T}$, *pak číslo* x_i *nazýváme* i-tá souřadnice vektoru $\mathbf{x}$.

V celém následujícím textu budeme také používat termín *skalár* místo *prvek tělesa* $\mathbf{T}$, bude-li z kontextu jasné, jaké těleso máme na mysli. A protože v této a několika příštích kapitolách budeme pracovat pouze s aritmetickými vektory, budeme také často vynechávat přívlastek aritmetický.

Vektory dimenze n nad tělesem $\mathbf{T}$ umíme sčítat a násobit skalárem. Připomňme si, že základní vlastnosti sčítání matic a součinu skaláru s maticí jsme shrnuli v Tvrzení **??** a Tvrzení **??**. Na tyto vlastnosti se budeme často odvolávat stejně jako na Tvrzení **??**

Definice 4.3 *Množinu všech aritmetických vektorů dimenze n nad tělesem* $\mathbf{T}$ *budeme nazývat* aritmetický vektorový prostor dimenze n nad tělesem $\mathbf{T}$ *a označovat ji* $\mathbf{T}^n$.

Definice 4.4 *Neprázdná podmnožina U aritmetického prostoru $\mathbf{T}^n$ se nazývá podprostor $\mathbf{T}^n$ pokud pro každé $\mathbf{x}, \mathbf{y} \in U$ platí, že také $\mathbf{x} + \mathbf{y} \in U$ a rovněž pro každé $\mathbf{x} \in U$ a každý skalár $a \in \mathbf{T}$ platí také $a\mathbf{x} \in U$.*

Jinak řečeno, množina U musí být uzavřená na sčítání vektorů a jejich násobení skalárem. Každý podprostor musí obsahovat nulový vektor $\mathbf{0} = 0\mathbf{x}$ pro libovolný vektor $\mathbf{x} \in U$. Jednoprvková množina $\{\mathbf{0}\}$ stejně jako celý prostor $\mathbf{T}^n$ jsou podprostory $\mathbf{T}^n$.

Tvrzení 4.1 *Pro každou matici $\mathbf{A}$ typu $m \times n$ nad tělesem $\mathbf{T}$ je množina všech řešení homogenní soustavy $\mathbf{Ax} = \mathbf{0}$ podprostor $\mathbf{T}^n$.*

Důkaz. Platí, že $\mathbf{A} \cdot \mathbf{0}_n = \mathbf{0}_n$ - množina řešení $\mathbf{Ax} = \mathbf{0}$ je neprázdná.
Je-li $\mathbf{Ax} = \mathbf{0}$ a $\mathbf{Ay} = \mathbf{0} \Rightarrow \mathbf{A}(\mathbf{x} + \mathbf{y}) = \mathbf{Ax} + \mathbf{Ay} = \mathbf{0}$.
Je-li $\mathbf{Ax} = \mathbf{0}$ a $a \in \mathbf{T} \Rightarrow \mathbf{A}(a\mathbf{x}) = a(\mathbf{Ax}) = \mathbf{0}$. □

Tvrzení 4.2 *Buď $\mathbf{T}$ libovolné těleso.*

1. *Pro každý podprostor U prostoru $\mathbf{T}^n$ platí $\mathbf{0} \in U$,*
2. *průnik podprostorů $\mathbf{T}^n$ je opět podprostor $\mathbf{T}^n$,*
3. *pro každou podmnožinu $X \subseteq \mathbf{T}^n$ existuje nejmenší (v uspořádání inkluzí) podprostor $\mathbf{T}^n$, který ji obsahuje.*

Důkaz.
1. $U \neq \emptyset$ a pro libovolný vektor $\mathbf{x} \in U$ platí $\mathbf{0x} = \mathbf{0} \in U$
2. Jsou-li $U_i, i \in I$ podprostory $\mathbf{T}^n$, potom $\bigcap_{i \in I} U_i$ má být podprostor $\mathbf{T}^n$

- $\mathbf{0} \in \bigcap_{i \in I} U_i \neq \emptyset$
- $\mathbf{x}, \mathbf{y} \in \bigcap_{i \in I} U_i \Rightarrow (\forall i \in I)(\mathbf{x}, \mathbf{y} \in U_i) \Rightarrow (\forall i \in I)(\mathbf{x} + \mathbf{y} \in U_i) \Rightarrow (\mathbf{x} + \mathbf{y}) \in \bigcap_{i \in I}$
- $\mathbf{x} \in \bigcap_{i \in I} U_i, a \in \mathbf{T} \Rightarrow (\forall i \in I)(\mathbf{x} \in U_i) \Rightarrow (\forall i \in I)(\forall a \in \mathbf{T})(a\mathbf{x} \in U_i) \Rightarrow a\mathbf{x} \in \bigcap_{i \in I} U_i$

3. Průnik všech podprostorů obsahujících X je podprostor $\mathbf{T}^n$ (podle 2.) a je obsažen v každém podprostoru $\mathbf{T}^n$, který obsahuje X. □

Definice 4.5 *Nejmenší podprostor $\mathbf{T}^n$ obsahující množinu $X \subseteq \mathbf{T}^n$ nazýváme* lineární obal množiny X *a označujeme* $\mathbf{L}(X)$.

Tvrzení 4.3 *Jsou-li X, Y podmnožiny $\mathbf{T}^n$, pak platí*

1. $X \subseteq \mathbf{L}(X)$,
2. *je-li* $X \subseteq Y$, *pak* $\mathbf{L}(X) \subseteq \mathbf{L}(Y)$,
3. $\mathbf{L}(\mathbf{L}(X)) = \mathbf{L}(X)$,
4. $\mathbf{L}(X) = \{a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + \cdots + a_k\mathbf{x}_k : \mathbf{x}_1, \ldots, \mathbf{x}_k \in X, a_1, \ldots, a_k \in \mathbf{T}\}$.

Důkaz.
1. Plyne z definice.
2. Platí $X \subseteq Y \subseteq \mathbf{L}(Y)$, tedy $\mathbf{L}(X) \subseteq \mathbf{L}(Y)$.
3. $\mathbf{L}(X) \subseteq \mathbf{L}(\mathbf{L}(X)$ (plyne z 1. dosadíme-li $X = \mathbf{L}(X)$); opačná inkluze plyne z toho, že $\mathbf{L}(X)$ je podprostor obsahující $\mathbf{L}(X)$
4. $\supseteq$: platí, že $a_1\mathbf{x}_1 + \cdots + a_k\mathbf{x}_k \in \mathbf{L}(X) \forall \mathbf{x}_1, \ldots, \mathbf{x}_k \in X$ a $\forall a_1, \ldots, a_k \in \mathbf{T}$ (protože $\mathbf{x} \in \mathbf{L}(X)$, pak $b\mathbf{x} \in \mathbf{L}(X) \forall b \in \mathbf{T}$).
$\subseteq$: k tomu stačí ukázat, že $\{a_1\mathbf{x}_1 + \cdots + a_k\mathbf{x}_k; k \geq 1; \mathbf{x}_1, \ldots, \mathbf{x}_k \in X; a_1, \ldots, a_k \in \mathbf{T}\} = U$ je podprostor $\mathbf{T}^n$.
Jsou-li $a_1\mathbf{x}_1 + \cdots + a_k\mathbf{x}_k$, $b_1\mathbf{y}_1 + \cdots + b_l\mathbf{y}_l$ prvky U,
potom $[(a_1\mathbf{x}_1 + \cdots + a_k\mathbf{x}_k) + (b_1\mathbf{y}_1 + \cdots + b_l\mathbf{y}_l)] \in U$
$a(a_1\mathbf{x}_1 + \cdots + a_k\mathbf{x}_k) = aa_1\mathbf{x}_1 + \cdots + aa_k\mathbf{x}_x \in U$
$\forall a \in \mathbf{T}\ \forall a_1\mathbf{x}_1 + \cdots + a_k\mathbf{x}_k \in U$ □

Definice 4.6 *Pro každou matici $\mathbf{A}$ typu $m \times n$ definujeme čtyři základní podprostory definované maticí $\mathbf{A}$:*

1. nulový prostor $\mathbf{N}(\mathbf{A})$ *jako podprostor $\mathbf{T}^n$ obsahující všechna řešení homogenní soustavy $\mathbf{Ax} = \mathbf{0}$,*
2. levý nulový prostor *jako podprostor* $\mathbf{N}(\mathbf{A}^T) \subseteq \mathbf{T}^m$,
3. sloupcový prostor $\mathbf{S}(\mathbf{A}) \subseteq \mathbf{T}^m$ *jako lineární obal sloupcových vektorů matice $\mathbf{A}$,*
4. řádkový prostor $\mathbf{R}(\mathbf{A}) \subseteq \mathbf{T}^n$ *jako podprostor* $\mathbf{S}(\mathbf{A}^T)$.

Definice 4.7 *Jsou-li X, Y podmnožiny $\mathbf{T}^n$, pak definujeme jejich součet $X + Y$ jako množinu $\{\mathbf{x} + \mathbf{y} : \mathbf{x} \in X, \mathbf{y} \in Y\}$.*

Tvrzení 4.4 *Součet podprostorů $\mathbf{T}^n$ je podprostor $\mathbf{T}^n$.*

Důkaz. $U, V \subseteq \mathbf{T}^n$ jsou podprostory $\mathbf{T}^n$

- $\mathbf{0} = \mathbf{0} + \mathbf{0} \in U + V \neq \emptyset$
- Jsou-li $\mathbf{x} + \mathbf{y} \in U + V$, $\mathbf{u} + \mathbf{v} \in U + V$
  $\mathbf{x}, \mathbf{u} \in U \to \mathbf{x} + \mathbf{u} \in U$, $\mathbf{y}, \mathbf{v} \in V \to \mathbf{y} + \mathbf{v} \in V$
  Tedy
  $(\mathbf{x} + \mathbf{u}) + (\mathbf{y} + \mathbf{v}) \in U + V$
  $(\mathbf{x} + \mathbf{y}) + (\mathbf{y} + \mathbf{v}) \in U + V$
- Je-li $a \in \mathbf{T}$, pak $a\mathbf{x} \in U$, $a\mathbf{y} \in V$
  $a\mathbf{x} + a\mathbf{y} \in U + V$
  $a(\mathbf{x} + \mathbf{y}) \in U + V$

□

Tvrzení 4.5 *Buď* $\mathbf{A}$ *libovolná matice typu* $m \times n$ *nad tělesem* $\mathbf{T}$ *a* $\mathbf{b} \in \mathbf{T}^m$. *Pak platí*

1. *jsou-li* $\mathbf{y}, \mathbf{z}$ *řešení soustavy* $\mathbf{Ax} = \mathbf{b}$, *pak* $\mathbf{z} - \mathbf{y} \in \mathbf{N}(\mathbf{A})$,
2. *jsou-li* $\mathbf{y}, \mathbf{z}$ *řešení soustavy* $\mathbf{Ax} = \mathbf{b}$, *pak existuje* $\mathbf{u} \in \mathbf{N}(\mathbf{A})$ *takové, že* $\mathbf{z} = \mathbf{y} + \mathbf{u}$,
3. *množina všech řešení soustavy* $\mathbf{Ax} = \mathbf{b}$ *se rovná* $\{\mathbf{y}\} + \mathbf{N}(\mathbf{A})$, *kde* $\mathbf{y}$ *je libovolné pevně zvolené řešení soustavy* $\mathbf{Ax} = \mathbf{b}$.

Důkaz.
1. $\mathbf{A}(\mathbf{z} - \mathbf{y}) = \mathbf{Az} - \mathbf{Ay} = \mathbf{b} - \mathbf{b} = \mathbf{0} \Rightarrow \mathbf{y} - \mathbf{z} \in \mathbf{N}(\mathbf{A})$
2. $\mathbf{z} = \mathbf{y} + (\mathbf{z} - \mathbf{y})$; $\mathbf{z} - \mathbf{y} = \mathbf{u} \in \mathbf{N}(\mathbf{A})$
3. Je-li prvek $\mathbf{y}$ řešením $\mathbf{Ax} = \mathbf{b}$ a $\mathbf{u} \in \mathbf{N}(\mathbf{A})$, potom $\mathbf{A}(\mathbf{y}+\mathbf{u}) = \mathbf{Ay}+\mathbf{Au} = \mathbf{b}+\mathbf{0} \Rightarrow \mathbf{y}+\mathbf{u}$ je řešením $\mathbf{Ax} = \mathbf{b}$, tedy každý prvek $\{\mathbf{y}\}+\mathbf{N}(\mathbf{A})$ je řešením $\mathbf{Ax} = \mathbf{b}$.
Naopak libovolné řešení rovnice $\mathbf{Ax} = \mathbf{b}$ lze vyjádřit ve tvaru $\mathbf{z} = \mathbf{y} + \mathbf{u}$, kde $\mathbf{u} \in \mathbf{N}(\mathbf{A})$ (podle 2.). □

Definice 4.8 *Platí-li* $U = \mathbf{L}(X)$ *pro* $X \subseteq \mathbf{T}^n$, *pak říkáme, že* X generuje *podprostor* U. *Je-li* $\mathbf{y} \in \mathbf{L}(X)$, *pak říkáme, že* $\mathbf{y}$ lineárně závisí *na* X.

Všimněme si, že podle Tvrzení **??**.3 vektor $\mathbf{y} \in \mathbf{T}^n$ lineárně závisí na $X \subseteq \mathbf{T}^n$ právě když lze $\mathbf{y}$ vyjádřit jako lineární kombinaci nějakých prvků z X.

Tvrzení 4.6 *Jsou-li* X, Y *podmnožiny* $\mathbf{T}^n$ *a* $Y \subseteq \mathbf{L}(X)$, *pak platí* $\mathbf{L}(X) = \mathbf{L}(X \cup Y)$.

Důkaz. $X \subseteq X \cup Y \Rightarrow \mathbf{L}(X) \subseteq \mathbf{L}(X \cup Y)$ podle Tvrzení **??**.2.
Je-li V podprostor $\mathbf{T}^n$ obsahující X, pak musím obsahovat i $\mathbf{L}(X) \supseteq Y$. Tedy $V \supseteq \mathbf{L}(X) \cup Y \supseteq X \cup Y$. Každý podprostor U, který obsahuje X, obsahuje i $X \cup Y$, tedy $\mathbf{L}(X) \supseteq \mathbf{L}(X \cup Y)$. □

Definice 4.9 *Množina vektorů $X \subseteq \mathbf{T}^n$ se nazývá* lineárně nezávislá *v $\mathbf{T}^n$ jestliže pro každé $k \geq 1$, každé vektory $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k \in X$ a každé skaláry $a_1, a_2, \ldots, a_k$ z rovnosti $a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + \cdots + a_k\mathbf{x}_k = \mathbf{0}$ plyne $a_1 = a_2 = \cdots = a_k = 0$. Množina, která není lineárně nezávislá, se nazývá* lineárně závislá *v $\mathbf{T}^n$.*

Je-li X lineárně nezávislá množina v $\mathbf{T}^n$, pak $\mathbf{0} \notin X$. Pokud $\mathbf{x} \in X$ pak $a\mathbf{x} \notin X$ pro libovolný skalár $a \neq 1$. Prázdná podmnožina je lineárně nezávislá v $\mathbf{T}^n$. Každá podmnožina lineárně nezávislé množiny v $\mathbf{T}^n$ je také lineárně nezávislůá v $\mathbf{T}^n$

Tvrzení 4.7 *Množina $X \subseteq \mathbf{T}^n$ je lineárně nezávislá v $\mathbf{T}^n$ právě když pro každý vektor $\mathbf{x} \in X$ platí $\mathbf{x} \notin \mathbf{L}(X \setminus \{\mathbf{x}\})$.*

Důkaz. $\rightarrow$ Sporem: Kdyby platilo $\mathbf{x} \in \mathbf{L}(X - \{\mathbf{x}\})$, pak by existovaly navzájem různé vektory $\mathbf{x}_1, \ldots, \mathbf{x}_k \in X - \{\mathbf{x}\}$ takové, že $\mathbf{x} = a_1\mathbf{x}_1 + \cdots + a_k\mathbf{x}_k$ pro $a_1, \ldots, a_k \in \mathbf{T}$, tedy $-1 \cdots \mathbf{x} + a_1\mathbf{x}_1 + \cdots + a_k\mathbf{x}_k\mathbf{0}$
-1 je nenulový koeficient, tj. spor s lieární nezávislostí množiny X. □

Věta 4.8 ***Steinitzova věta o výměně***
Nechť U je podprostor $\mathbf{T}^n$, $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\} \subseteq U$ je množina lineárně nezávislá v $\mathbf{T}^n$, a $\{\mathbf{y}_1, \ldots, \mathbf{y}_l\} \subseteq U$ generuje U. Pak platí $k \leq l$ a po vhodném přeuspořádání vektorů $\mathbf{y}_j$ množina $\{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}_{k+1}, \ldots, \mathbf{y}_l\}$ generuje podprostor U.

Důkaz. Indukcí podle k.
1. $k = 1$, $\mathbf{x}_1 \in U$, $\mathbf{x}_1 \neq \mathbf{0}$ (je lineárně nezávislá).
$\mathbf{L}(\{\mathbf{y}_1, \ldots, \mathbf{y}_l\}) = U$, tedy $\mathbf{x}_1 = a_1\mathbf{y}_1 + \cdots + a_l\mathbf{y}_l$ pro $a_1, \ldots, a_l \in \mathbf{T}$.
Protože $\mathbf{x}_1 \neq \mathbf{0}$, existuje $a_i \neq 0$. Přeindexováním dosáhneme toho, že $a_1 \neq 0$.
Vyjádříme $\mathbf{y}_1 = a_1^{-1}(\mathbf{x}_1 - a_2\mathbf{y}_2 - \cdots - a_l\mathbf{y}_l)$
Tedy $l \geq 1$ a $\mathbf{y}_1 \in \mathbf{L}(\{\mathbf{x}_1, \mathbf{y}_2, \ldots, \mathbf{y}_l\}) = \mathbf{L}(\{\mathbf{x}_1, \mathbf{y}_1, \ldots, \mathbf{y}_l\}) = \cdots$
$\cdots = \mathbf{L}(\{\mathbf{y}_1, \ldots, \mathbf{y}_l\}) = U$
Pozn.: První dvě rovnosti opravňuje Tvrzení 4.6
2. Nechť $k \geq 2$.
O tvrzení platí: $\{\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}\} \subseteq U$, tj. $k - 1 \leq l$ a po přeindexování

$\{\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{y}_k, \ldots, \mathbf{y}_l\}$ generuje U.
$\mathbf{x}_k \in U$ ...můžeme vyjádřit $\mathbf{x}_k$ jako lineární kombinaci $\{\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}\}$
$\mathbf{x}_k = b_1\mathbf{x}_1 + \cdots + b_{k-1}\mathbf{x}_{k-1} + b_k\mathbf{y}_k + \cdots + b_l\mathbf{y}_l$
Kdyby $b_k = b_{k+1} = \cdots = b_l = 0$, bylo by $\mathbf{x}_k = b_1\mathbf{x}_1 + \cdots + b_{k-1}\mathbf{x}_{k-1}$ (spor s tím, že $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ je lineárně nezávislá). Tedy existuje alespoň jedno $b_j \neq 0$ pro $j = k, \ldots, l$, proto $k \leq l$. Po přeindexování můžeme předpokládat, že $b_k \neq 0$, pak můžeme vyjádřit:
$\mathbf{y}_k = b_k^{-1}(\mathbf{x}_k - b_1\mathbf{x}_1 - \cdots - b_{k-1}\mathbf{x}_{k-1} - b_{k+1}\mathbf{y}_{k+1} - \cdots - b_l\mathbf{y}_l)$
Tedy $\mathbf{y}_k \in \mathbf{L}(\{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}_{k+1}, \ldots \mathbf{y}_l\}) = \mathbf{L}(\{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}_k, \mathbf{y}_{k+1}, \ldots \mathbf{y}_l\}) = \mathbf{L}(\{\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{y}_k, \mathbf{y}_{k+1}, \ldots \mathbf{y}_l\}) = U$
Pozn.: Rovnosti opět platí podle Tvrzení 4.6. □

Definice 4.10 *Jestliže množina $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\} \subseteq U$ generuje podprostor $U \subseteq \mathbf{T}^n$ a je lineárně nezávislá v $\mathbf{T}^n$, pak ji nazýváme* báze U.

Příklad 4.1 Standardní báze v $\mathbf{T}^n$.

Věta 4.9 *Každý podprostor $U \subseteq \mathbf{T}^n$ má nějakou bázi. Všechny báze podprostoru U mají stejný počet prvků menší nebo rovný n, přičemž rovnost nastává právě když $U = \mathbf{T}^n$.*

Důkaz.

Pomocné tvrzení: Je-li množina vektorů $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\} \in U$ lineárně nezávislá a $\mathbf{L}(\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}) \subsetneq U$, potom existuje $\mathbf{x}_{k+1} \in U - \mathbf{L}(\{\mathbf{x}_1, \ldots, \mathbf{x}_k\})$ takové, že $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\, \mathbf{x}_{k+1}\}$ je lineárně nezávislá.
Důkaz: Nechť $\mathbf{x}_{k+1} \in U - \mathbf{L}(\{\mathbf{x}_1, \ldots, \mathbf{x}_k\})$ a $a_1\mathbf{x}_1 + \cdots + a_k\mathbf{x}_k + a_{k+1}\mathbf{x}_{k+1} = \mathbf{0}$ pro $a_1, \ldots, a_{k+1} \in \mathbf{T}$.
Kdyby $a_{k+1} = 0$, platilo by $\mathbf{x}_{k+1} = -a_{k+1}^{-1}(a_+\mathbf{x}_1 + \ldots + a_k\mathbf{x}_k)$, tj. spor s volbou $\mathbf{x}_{k+1} \in U - \mathbf{L}(\{\mathbf{x}_1, \ldots, \mathbf{x}_k\})$. Tedy $a_{k+1} = 0$ a z lineární nezávislosti $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ plyne $a_1 = a_2 = \cdots = a_k = 0$.

Je-li $U = \{\mathbf{0}\}$ je $\emptyset$ báze.
Pokud $U \neq \{\mathbf{0}\}$ zvolíme $\mathbf{0} \neq \mathbf{x}_1 \in U$, $\{\mathbf{x}_1\}$ je lineárně nezávislá.
Pokud $\mathbf{L}(\{\mathbf{x}_1\}) = U$, je $\{\mathbf{x}_1\}$ báze U.
Pokud $\mathbf{L}(\{\mathbf{x}_1\}) \subsetneq U$, existuje $\mathbf{x}_2 \in U - \mathbf{L}(\{\mathbf{x}_1\})$ tak, že $\{\mathbf{x}_1, \mathbf{x}_2\}$ je lineárně nezávislá.

Po $k \leq n$ krocích najdeme lineárně nezávislou množinu $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ takovou, že $\mathbf{L}(\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}) = U$.
Pokud by $\mathbf{L}(\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}) \subsetneq U$, našli bychom množinu $\{\mathbf{x}_1, \ldots, \mathbf{x}_{n+1}\} \subseteq U \subseteq \mathbf{T}^n$, to by byl spor s tím, že v $\mathbf{T}^n$ existuje (standardní) báze, která má n prvků, tedy každá lineárně nezávislá množina v U má nejvýše n prvků.

- Jsou-li $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ a $\{\mathbf{y}_1, \ldots, \mathbf{y}_l\}$ báze v U, pak podle Steinitzovy věty $k \leq n$, stejně tak $l \leq n$.
- Je-li $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ báze v U, víme, že $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ je báze v $\mathbf{T}^n$, pak podle Steinitzovy věty je $k \leq n$.
- V $\mathbf{T}^n$ existuje báze velikosti n - standardní báze. Je-li U podprostor v $\mathbf{T}^n$ a $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ je báze v U, pak $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ je lineárně nezávislá v $\mathbf{T}^n$. Pokud by $\mathbf{L}(\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}) \subsetneq \mathbf{T}^n$, použijeme pomocné tvrzení pro $U = \mathbf{T}^n$ k nalezení $\mathbf{x}_{n+1}$ takové, že $\{\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{x}_{n+1}\}$ je lineárně nezávislá v $\mathbf{T}^n$ - spor se Steinitzovou větou.

□

Tvrzení 4.10 *Pro podmnožinu $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ podprostoru U prostoru $\mathbf{T}^n$ jsou následující tři podmínky ekvivalentní*

1. *$\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ je báze U,*
2. *$\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ je minimální (co do počtu prvků) generující množina v U,*
3. *$\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ je maximální (co do počtu prvků) lineárně nezávislá podmnožina U.*

Důkaz.
$1 \to 2$ $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ generuje U, pokud $\mathbf{L}(\{\mathbf{y}_1, \ldots, \mathbf{y}_l\}) = U$, plyne ze Steinitzovy věty, že $k \leq l$.
$2 \to 3$ Chceme dokázat, že $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ je lineárně nezávislá v $\mathbf{T}^n$. Kdyby nebyla, existovalo by $\mathbf{x}_i$, $(1 \leq i \leq k)$, které by bylo lineární kombinací ostatních vektorů, tedy $\mathbf{x}_i \in \mathbf{L}(\{\mathbf{x}_1, \ldots, \mathbf{x}_{i-1}, \mathbf{x}_{i+1}, \ldots, \mathbf{x}_k\})$ (Tvrzení **??**).
Podle Tvrzení **??** platí, že $\mathbf{L}(\{\mathbf{x}_1, \ldots, \mathbf{x}_{i-1}, \mathbf{x}_{i+1}, \ldots, \mathbf{x}_k\}) = \mathbf{L}(\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}) = U$ - spor s tím, že $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ je minimální generující množina.
$3 \to 1$ Chceme dokázat, že $\mathbf{L}(\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}) = U$. Kdyby ne, tak podle pomocného tvrzení z důkazu Věty **??** najdeme větší lineárně nezávislou množinu v U - spor s maximalitou $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$. □

Věta 4.11 *Je-li U podprostor $\mathbf{T}^n$ a $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\} \subseteq U$ je lineárně nezávislá v $\mathbf{T}^n$, pak lze $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ rozšířit do báze U.*

Důkaz. Zvolíme bázi $\{\mathbf{y}_1, \ldots, \mathbf{y}_l\}$ v U. Podle Steinitzovy věty je $k \leq l$ a po přeuspořádání platí, že $\{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}_{k+1}, \ldots, \mathbf{y}_l\}$ generuje U. Podle Tvrzení **??** je to báze. □

Definice 4.11 *Počet prvků báze podprostoru $U \subseteq \mathbf{T}^n$ nazýváme* dimenze *U a značíme* $\dim U$.

Tvrzení 4.12 *Jsou-li $U \subseteq V$ podprostory $\mathbf{T}^n$, pak platí* $\dim U \leq \dim V$.

Důkaz. Buď $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ báze v U (tedy je lineárně nezávislá v U, generuje U a navíc $\dim U = k$). Protože $U \subseteq V$, je $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ lineárně nezávislá ve V. Buď $\{\mathbf{y}_1, \ldots, \mathbf{y}_l\}$ báze ve V (tedy je lineárně nezávislá ve V, generuje V a navíc $\dim V = l$). Podle Věty **??** platí, že $k \leq l$, tedy $\dim U \leq \dim V$. □

Věta 4.13 ***O dimenzi součtu a průniku podprostorů***
Jsou-li U, V podprostory $\mathbf{T}^n$, pak platí

$$\dim(U \cap V) + \dim(U + V) = \dim U + \dim V.$$

Důkaz. Zvolíme bázi $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ v $U \cap V$.
Podle Věty **??** ji rozšíříme do $\{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{x}_{k+1}, \ldots, \mathbf{x}_l\}$ báze v U.
Podle Věty **??** ji rozšíříme do $\{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}_{k+1}, \ldots, \mathbf{y}_m\}$ báze ve V.
Tedy: $\dim(U \cap V) = k$, $\dim U = l$, $\dim V = m$.
Chceme najít bázi v $U+V$, která má dimenzi $m+l-k$. Sjednocení $\{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{x}_{k+1}, \ldots, \mathbf{x}_l\}$ a $\{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}_{k+1}, \ldots, \mathbf{x}_m\}$ má přesně $m + l - k$ prvků.
Víme, že $\{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{x}_{k+1}, \ldots, \mathbf{x}_l, \mathbf{y}_{k+1}, \ldots, \mathbf{y}_m\} \subseteq U + V$, cheme dokázat, že je to báze $U + V$.
1. Chceme dokázat, že generuje $U + V$.
Tedy že $\mathbf{L}(\{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{x}_{k+1}, \ldots, \mathbf{x}_l, \mathbf{y}_{k+1}, \ldots, \mathbf{y}_m\}) = U + V$.
Inkluze $\subseteq$ je triviální.
$\supseteq$: Buď $\mathbf{z} \in U + V$, platí, že $\mathbf{z} = \mathbf{x} + \mathbf{y}$, kde $\mathbf{x} \in U$, $\mathbf{y} \in V$.
$\{\mathbf{x}_1, \ldots, \mathbf{x}_l\}$ je báze U, tedy

$$\mathbf{x} = \sum_{i=1}^{l} a_i \mathbf{x}_i$$

$\{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}_{k+1}, \ldots, \mathbf{y}_m\}$ je báze ve V, tedy

$$\mathbf{y} = \sum_{i=1}^{k} b_i \mathbf{x}_i + \sum_{j=k+1}^{m} c_j \mathbf{y}_j$$

$$\mathbf{x} + \mathbf{y} = \sum_{i=1}^{k} (a_i + b_i)\mathbf{x}_i + \sum_{i=k+1}^{l} a_i \mathbf{x}_i + \sum_{j=k+1}^{m} c_j \mathbf{y}_j$$

Tedy $\mathbf{x} + \mathbf{y} \in \mathbf{L}(\{\mathbf{x}_1, \ldots, \mathbf{x}_l, \mathbf{y}_{k+1}, \ldots, \mathbf{y}_m\})$.
2. Chceme dokázat, že je lineárně nezávislá. Je-li

$$\sum_{i=1}^{l} a_i \mathbf{x}_i + \sum_{j=k+1}^{m} b_j \mathbf{y}_j = \mathbf{0}$$

Platí, že $\sum_{i=1}^{l} a_i \mathbf{x}_i \in U$, $\sum_{j=k+1}^{m} b_j \mathbf{y}_j \in V$, proto prvek:

$$\mathbf{w} = \sum_{i=1}^{l} a_i \mathbf{x}_i \in U = -\sum_{j=k+1}^{m} b_j \mathbf{y}_j \in U + V$$

Protože $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ je báze $U \cap V$, lze vyjádřit

$$\mathbf{w} = \sum_{i=1}^{k} b_i \mathbf{x}_i = -\sum_{j=k+1}^{m} b_j \mathbf{y}_j$$

Tedy

$$\sum_{i=1}^{k} b_i \mathbf{x}_i + \sum_{j=k+1}^{m} b_j \mathbf{y}_j = \mathbf{0}$$

Protože $\{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}_{k+1}, \ldots, \mathbf{y}_m\}$ je báze V (tedy lineárně nezávislá), platí, že $b_1 = b_2 \cdots = b_m = 0 \rightarrow \mathbf{w} = \mathbf{0}$, tedy

$$\mathbf{w} = \sum_{i=1}^{l} a_i \mathbf{x}_i = \mathbf{0}$$

Protože $\{\mathbf{x}_1, \ldots, \mathbf{x}_l\}$ je báze U, platí $a_1 = a_2 = \cdots = a_l = 0$.
Proto $\{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}_{k+1}, \ldots, \mathbf{y}_m\}$ je lineárně nezávislá. □

Tvrzení 4.14 *Je-li* $\mathbf{A}$ *matice typu* $m \times n$ *nad tělesem* $\mathbf{T}$, *je-li* $\mathbf{E}$ *regulární matice řádu* m, *a* $1 \leq j_1 < j_2 < \cdots < j_k \leq n$, *pak platí*

1. *množina* $\{\mathbf{A}_{*j_1}, \mathbf{A}_{*j_2}, \ldots, \mathbf{A}_{*j_k}\}$ *je lineárně nezávislá v* $\mathbf{T}^m$ *právě když množina* $\{(\mathbf{EA})_{*j_1}, (\mathbf{EA})_{*j_2}, \ldots, (\mathbf{EA})_{*j_k}\}$ *je lineárně nezávislá v* $\mathbf{T}^m$,

2. *množina* $\{\mathbf{A}_{*j_1}, \mathbf{A}_{*j_2}, \ldots, \mathbf{A}_{*j_k}\}$ *generuje* $\mathbf{S}(\mathbf{A})$ *právě když množina* $\{(\mathbf{EA})_{*j_1}, (\mathbf{EA})_{*j_2}, \ldots, (\mathbf{EA})_{*j_k}\}$ *generuje* $\mathbf{S}(\mathbf{EA})$,

3. *množina* $\{\mathbf{A}_{*j_1}, \mathbf{A}_{*j_2}, \ldots, \mathbf{A}_{*j_k}\}$ *je báze sloupcového prostoru* $\mathbf{S}(\mathbf{A})$ *právě když množina* $\{(\mathbf{EA})_{*j_1}, (\mathbf{EA})_{*j_2}, \ldots, (\mathbf{EA})_{*j_k}\}$ *je báze* $\mathbf{S}(\mathbf{EA})$,

4. $\dim \mathbf{S}(\mathbf{A}) = \dim \mathbf{S}(\mathbf{EA})$

5. $\mathbf{R}(\mathbf{A}) = \mathbf{R}(\mathbf{EA})$.

Důkaz. Za pomocí Tvrzení 2.9.
1. $\rightarrow$: Nechť $\{\mathbf{A}_{*j_1}, \ldots, \mathbf{A}_{*j_k}\}$ je lineárně nezávislá v $\mathbf{T}^n$.
$a_1\mathbf{A}_{*j_1} + \cdots + a_k\mathbf{A}_{*j_k} = \mathbf{0}$
Podle Tvrzení **??** platí, že $a_1(\mathbf{eA})_{*j_1} + \cdots + a_k(\mathbf{EA})_{*j_k} = \mathbf{0}$.
Protože $\{\mathbf{A}_{*j_1}, \ldots, \mathbf{A}_{*j_k}\}$ je lineárně nezávislá, platí $a_1 = a_2 = \cdots = a_k = 0$
, tedy $\{(\mathbf{EA})_{*j_1}, \ldots, (\mathbf{EA})_{*j_k}\}$ je lineárně nezávislá.
$\leftarrow$: Je-li $\{(\mathbf{EA})_{*j_1}, \ldots, (\mathbf{EA})_{*j_k}\}$ lineárně nezávislá v $\mathbf{T}^n$ a
$a_1(\mathbf{eA})_{*j_1} + \cdots + a_k(\mathbf{EA})_{*j_k} = \mathbf{0}$,
pak podle Tvrzení **??** platí $a_1\mathbf{EA}_{*j_1} + \cdots + a_k\mathbf{EA}_{*j_k} = \mathbf{0}$.
$a_1\mathbf{E}^{-1}\mathbf{EA}_{*j_1} + \cdots + a_k\mathbf{E}^{-1}\mathbf{EA}_{*j_k} = \mathbf{E}^{-1}\mathbf{0}$
$a_1\mathbf{A}_{*j_1} + \cdots + a_k\mathbf{A}_{*j_k} = \mathbf{0}$
Z lineární nezávislosti $\{(\mathbf{EA})_{*j_1}, \ldots, (\mathbf{EA})_{*j_k}\}$ vyplývá,
že $a_1 = a_2 = \cdots = a_k = 0$, tedy i $\{\mathbf{A}_{*j_1}, \ldots, \mathbf{A}_{*j_k}\}$ je lineárně nezávislá.
2. $\rightarrow$ Pokud $\{\mathbf{A}_{*j_1}, \ldots, \mathbf{A}_{*j_k}\}$ generuje $\mathbf{S}(\mathbf{A})$, existuje pro každé $j \neq j_1, \ldots, j_k$
vyjádření
$\mathbf{A}_{*j} = b_1\mathbf{A}_{*j_1} + \cdots + b_k\mathbf{A}_{*j_k}$, tedy

$$\mathbf{0} = -\mathbf{A}_{*j} + \sum_{i=1}^{k} b_i\mathbf{A}_{*j_i}$$

Podle tvrzení 2.9 platí, že

$$\mathbf{0} = -(\mathbf{EA})_{*j} + \sum_{i=1}^{k} b_i(\mathbf{EA})_{*j_i}$$

j-tý sloupec je lineární kombinací vybraných sloupců, proto $\{(\mathbf{EA})_{*j_1}, \ldots, (\mathbf{EA})_{*j_k}\}$
generuje $\mathbf{S}(\mathbf{EA})$.
$\leftarrow$: analogicky jako v prvním důkazu pouze přenásobíe $\mathbf{E}^{-1}$ zleva.

3. Plyne ihned z 1, 2.
4. Plyne ihned z 3.
5. Plyne z Věty **??**.2: Každý řádek v $\mathbf{EA}$ je lineární kombinací řádků matice $\mathbf{A}$, proto $\{(\mathbf{EA})_{i*} \in \mathbf{L}(\{\mathbf{A}_{1*}, \ldots, \mathbf{A}_{m*}\})$, tedy také $\mathbf{R}(\mathbf{EA}) = \mathbf{L}(\{(\mathbf{EA})_{1*}, \ldots, (\mathbf{EA})_{m*}\}) \subseteq \mathbf{L}(\{\mathbf{A}_{1*}, \ldots, \mathbf{A}_{m*}\})$.
$\supseteq$: Postupujeme opačně pomocí násobení $\mathbf{E}^{-1}$ zleva. □

Tvrzení 4.15 *Předpokládáme, že* $\mathbf{A}$ *je matice typu* $m \times n$ *a* $\mathbf{B}$ *je matice v řádkově odstupňovaném tvaru, kterou dostaneme z* $\mathbf{A}$ *pomocí elementárních řádkových operací. Následující podmínky jsou ekvivalentní:*

1. *vektor* $\mathbf{B}_{*j}$ *je bázový sloupec matice* $\mathbf{B}$,
2. *vektor* $\mathbf{B}_{*j}$ *není lineárně závislý na předchozích sloupcových vektorech* $\mathbf{B}_{*1}, \mathbf{B}_{*2}, \ldots, \mathbf{B}_{*j-1}$,
3. *vektor* $\mathbf{A}_{*j}$ *není lineárně závislý na předchozích sloupcových vektorech* $\mathbf{A}_{*1}, \mathbf{A}_{*2}, \ldots, \mathbf{A}_{*j-1}$.

Důkaz. Existuje regulární matice $\mathbf{E}$ řádu n taková, že $\mathbf{B} = \mathbf{EA}$.
$2 \leftrightarrow 3$ plyne z Tvrzení **??**.2.
$1 \rightarrow 2$: Indexy bázových sloupců v $\mathbf{B}$ jsou $1 \leq j_1 \leq \cdots \leq j_k \leq n$, víme, že $b_{mj_m} \neq 0$, $b_{mj} = 0\ \forall j < j_m$ (z definice řádkově odstupňovaného tvaru).
Lineární kombinace $b_{mj} = 0$, ale $b_{mj_m} \neq 0$, tedy

$$\sum_{i=1}^{j_{m-1}} a_i b_{mi} \neq \mathbf{B}_{*j_m}$$

$2 \leftarrow 1$ sporem: Je-li $\mathbf{B}_{*j}$ nebázový sloupec, pak
a. $j < j_1$, pak $\mathbf{B}_{*j} = \mathbf{0}$, tedy je lineární kombinací předchozích sloupců.
b. $j_m < j < j_{m+1}$, v tomto případě je $\mathbf{B}_{*j}$ lineární kombinací sloupců $\mathbf{B}_{*j_1}, \ldots, \mathbf{B}_{*j_m}$, potřebujeme najít $a_1, \ldots, a_m \in \mathbf{T}$ tak, že
$a_1\mathbf{B}_{*j_1} + \ldots + a_m\mathbf{B}_{*j_m} = \mathbf{B}_{*j}$

$$\left(\begin{array}{c|c|c} \mathbf{B}_{*j_1} & \cdots & \mathbf{B}_{*j_m} \end{array} \right) \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} = \mathbf{B}_{*j}$$

Tuto soustavu řešíme pomocí zpětné substituce.
c. $j > j_k$ analogicky jako b. □

Definice 4.12 *Je-li* $\mathbf{A}$ *matice typu* $m \times n$*, pak sloupcový vektor* $\mathbf{A}_{*j}$ *nazýváme* bázový sloupec matice $\mathbf{A}$*, jestliže není lineárně závislý na předchozích sloupcových vektorech* $\mathbf{A}_{*1}, \mathbf{A}_{*2}, \ldots, \mathbf{A}_{*j-1}$.

Definice 4.13 *Řekneme, že matice* $\mathbf{B} = (b_{ij})$ *typu* $m \times n$ *je v* redukovaném řádkově odstupňovaném tvaru*, jestliže existuje nezáporné celé číslo* $k \leq m$ *a čísla* $1 \leq j_1 < j_2 < \cdots < j_m \leq n$ *taková, že platí*

1. *pro každé* $i > k$ *platí* $\mathbf{B}_{i*} = \mathbf{0}$*, tj. všechny tyto řádky jsou nulové,*
2. *pro každé* $i = 1, 2, \ldots, k$ *platí* $b_{ij_i} = 1$*,*
3. *pro každé* $i = 1, 2, \ldots, k$ *a každé* $j < j_i$ *platí* $b_{ij} = 0$*,*
4. *pro každé* $l = 1, 2, \ldots, k$ *a každé* $i = 1, \ldots, j_l - 1$ *platí* $b_{ij_l} = 0$.

Tvrzení 4.16 *Každou matici* $\mathbf{A}$ *typu* $m \times n$ *nad tělesem* $\mathbf{T}$ *lze převést pomocí elementárních řádkových úprav do matice* $\mathbf{B}$*, která je v redukovaném řádkově odstupňovaném tvaru.*

Důkaz. Pomocí Gaussovy eliminace převedeme matici $\mathbf{A}$ na matici $\mathbf{B}$, která je v řádkově odstupňovaném tvaru. Označíme $j_1, \ldots, j_k$ indexy bázových sloupců. Poté $\forall i = 1, \ldots, k$ vynásobíme i-tý řádek číslem $b_{ij_i}^{-1}$. Poté $\forall m = 1, \ldots, k$ odečteme vhodný násobek m-tého řádku od řádku nad ním, abychom vynulovali všechny prvky na místech (i, j_m) pro $i = 1, \ldots, j_{m-1}$. □

Věta 4.17 *Pro každou matici* $\mathbf{A}$ *typu* $m \times n$ *nad tělesem* $\mathbf{T}$ *platí*

$$\dim \mathbf{S}(\mathbf{A}) = \dim \mathbf{R}(\mathbf{A}).$$

Důkaz. Najdeme regulární matici $\mathbf{E}$ řádu m takovou, že matice $\mathbf{B} = \mathbf{EA}$ je v redukovaném řádkově odstupňovaném tvaru. Taková matice existuje podle Tvrzení **??**, Tvrzení **??** a Tvrzení **??**.1.

Pro matici $\mathbf{B}$ platí rovnost $\dim \mathbf{S}(\mathbf{B}) = \dim \mathbf{R}(\mathbf{B})$. Podle Tvrzení **??**.4 platí $\dim \mathbf{S}(\mathbf{B}) = \dim \mathbf{S}(\mathbf{EA}) = \dim \mathbf{S}(\mathbf{A})$.

Protože $\mathbf{R}(\mathbf{B}) = \mathbf{R}(\mathbf{EA}) = \mathbf{R}(\mathbf{A})$, platí také $\dim \mathbf{R}(\mathbf{B}) = \dim \mathbf{R}(\mathbf{A})$. Stačí dokázat, že $\dim \mathbf{R}(\mathbf{B}) = \dim \mathbf{S}(\mathbf{B})$.
Bázové sloupce $\mathbf{B}_{*j_i} = \mathbf{e}_i$ jsou prvky standardní báze v $\mathbf{T}^m$, tedy jsou lineárně nezávislé. Podle Tvrzení **??**.2 je každý nebázový sloupec lineární kombinací bázových sloupců. To znamená, že bázové sloupce generují $\mathbf{S}(\mathbf{B})$,

jsou lineárně nezávislé, tedy tvoří bázi $\mathbf{S}(\mathbf{B})$, tedy $\dim \mathbf{S}(\mathbf{B}) = k$ (počtu bázových sloupců).
Nenulové řádky matice $\mathbf{B}$ jsou lineárně nezávislé (jsou prvky standardní báze v $\mathbf{T}^n$, a generují $\mathbf{R}(\mathbf{B})$, tedy tvoří bázi, proto $\dim \mathbf{R}(\mathbf{B}) = k$. □

Definice 4.14 *Číslo* $\dim \mathbf{S}(\mathbf{A})$ *nazýváme* hodnost matice $\mathbf{A}$ *a označujeme jej* $r(\mathbf{A})$.

Důsledek 4.18 *Pro každou matici* $\mathbf{A}$ *nad tělesem* $\mathbf{T}$ *platí*

1. $r(\mathbf{A}) = r(\mathbf{A}^T)$,
2. $r(\mathbf{A})$ *se rovná počtu nenulových řádků v matici v řádkově odstupňovaném tvaru, kterou dostaneme z* $\mathbf{A}$ *pomocí elementárních řádkových operací.*

Věta 4.19 *Následující podmínky pro čtvercovou matici* $\mathbf{A}$ *řádu* n *jsou ekvivalentní:*

1. $\mathbf{A}$ *je regulární,*
2. *sloupcové vektory matice* $\mathbf{A}$ *jsou lineárně nezávislé,*
3. *řádkové vektory matice* $\mathbf{A}$ *jsou lineárně nezávislé,*
4. $r(\mathbf{A}) = n$.

Důkaz.
$1 \to 4$ $\mathbf{A}$ je regulární, z Věty**??**.4 plyne, že v matici v řádkově odstupňovaném tvaru, kterou dostanemem $\mathbf{A}$ pomocí Gaussovy eliminace jsou všechny řádky nenulové. Podle Důsledku **??**.2 je $r(\mathbf{A}) = n$.
$4 \to 1$ Je-li $r(\mathbf{A}) = n$, jsou všechny řádky v matici v řádkově odstupňovaném tvaru, kterou dostaneme z $\mathbf{A}$ pomocí elementárních řádkových úprav, nenulové (podle Důsledku **??**.2), tedy matice je regulární (podle Věty **??**.4).
$4 \to 3$ Z $n = r(\mathbf{A}) = \dim \mathbf{L}(\mathbf{A}_{1*}, \ldots, \mathbf{A}_{n*})$ vyplývá, že $\{\mathbf{A}_{1*}, \ldots, \mathbf{A}_{n*}\}$ je minimální generující množina v $\mathbf{L}(\mathbf{A}_{1*}, \ldots, \mathbf{A}_{n*})$, tedy je báze, tedy lineárně nezávislá podle Tvrzení **??**.2.
$3 \to 4$ Jsou-li $\mathbf{A}_{1*}, \ldots, \mathbf{A}_{n*}$ lineárně nezávislé, tvoří bázi $\mathbf{R}(\mathbf{A})$, protože jej generují. Proto $\dim \mathbf{R}(\mathbf{A}) = n$.
$4 \leftrightarrow 2$ Stejně jako v předchozím případě, protože $r(\mathbf{A}) = \dim \mathbf{S}(\mathbf{A})$ (z definice $r(\mathbf{A})$). □

Tvrzení 4.20 *Je-li* $\mathbf{A}$ *matice typu* $m \times n$ *a* $\mathbf{B}$ *matice typu* $n \times p$*, pak platí*

$$r(\mathbf{AB}) \leq r(\mathbf{A}), r(\mathbf{B}).$$

Důkaz. Každý sloupec $(\mathbf{AB})*k$ je lineární kombinací sloupců matice $\mathbf{A}$ (podle Věty **??**.1). Tedy $(\mathbf{AB})_{*k} \in \mathbf{L}(\mathbf{A}_{*1}, \ldots, \mathbf{A}_{*n})$, proto $\mathbf{L}(\mathbf{A}_{*1}, \ldots, \mathbf{A}_{*n}) \in \mathbf{L}((\mathbf{AB})_{*1}, \ldots, (\mathbf{AB})_{*n})$.
Tedy $\mathbf{S}(\mathbf{AB}) \subseteq \mathbf{S}(\mathbf{A}) \Rightarrow \dim \mathbf{S}(\mathbf{AB}) \leq \dim \mathbf{S}(\mathbf{A}) \Rightarrow r(\mathbf{AB}) \leq r(\mathbf{A})$.
Podobě i $r(\mathbf{AB}) \leq r(\mathbf{B})$. Stačí použít rovností $r(\mathbf{AB}) = \dim \mathbf{R}(\mathbf{AB})$, $r(\mathbf{B}) = \dim \mathbf{R}(\mathbf{B})$. Z Věty **??**.2 máme $\mathbf{R}(\mathbf{AB}) \subseteq \mathbf{R}(\mathbf{B})$, tedy $\dim \mathbf{R}(\mathbf{AB}) \leq \dim(\mathbf{B}) \Rightarrow r(\mathbf{AB}) \leq r(\mathbf{B})$. □

Tvrzení 4.21 *Je-li* $\mathbf{A}, \mathbf{B}$ *matice typu* $m \times n$*, pak platí*

$$r(\mathbf{A}+\mathbf{B}) \leq r(\mathbf{A}) + r(\mathbf{B}) - \dim(\mathbf{S}(\mathbf{A}) \cap \mathbf{S}(\mathbf{B})) \leq r(\mathbf{A}) + r(\mathbf{B}).$$

Důkaz.

$$(\mathbf{A}+\mathbf{B})_{*k} = \mathbf{A}_{*k} + \mathbf{B}_{*k} \in \mathbf{S}(\mathbf{A}) + \mathbf{S}(\mathbf{B})$$

$$\mathbf{S}(\mathbf{A}+\mathbf{B}) = \mathbf{L}((\mathbf{A}_{*1} + \mathbf{B}_{*1}), \ldots, (\mathbf{A}_{*n} + \mathbf{B}_{*n})) \subseteq \mathbf{S}(\mathbf{A}) + \mathbf{S}(\mathbf{B})$$

$$r(\mathbf{A}+\mathbf{B}) = \dim \mathbf{S}(\mathbf{A}+\mathbf{B}) \leq \dim(\mathbf{S}(\mathbf{A}) + \mathbf{S}(\mathbf{B})) = \cdots$$

Podle Věty **??**

$$\cdots = \dim \mathbf{S}(\mathbf{A}) + \dim \mathbf{S}(\mathbf{B}) - dim(\mathbf{S}(\mathbf{A}) \cap \mathbf{S}(\mathbf{B})) \leq r(\mathbf{A}) + r(\mathbf{B})$$

□

Věta 4.22 *Pro každou matici* $\mathbf{A}$ *typu* $m \times n$ *platí*

$$\dim \mathbf{N}(\mathbf{A}) + r(\mathbf{A}) = n.$$

Důkaz. Víme, že $\mathbf{N}(\mathbf{A}) \subseteq \mathbf{T}^n$, zvolíme bázi $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ v $\mathbf{N}(\mathbf{A})$, doplníme ji do báze $\mathbf{T}^n$ $\{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}_1, \ldots, \mathbf{y}_{n-k}\}$ podle Věty **??**. Dokážeme, že $\{\mathbf{A}\mathbf{y}_1, \ldots, \mathbf{A}\mathbf{y}_{n-k}\}$ tvoří bázi $\mathbf{S}(\mathbf{A})$:
1. generují: $\mathbf{S}(\mathbf{A}) = \mathbf{L}(\mathbf{A}_{*1}, \ldots, \mathbf{A}_{*n})$.
Je-li $\mathbf{y} \in \mathbf{S}(\mathbf{A})$

$$\mathbf{y} = \sum_{j=1}^{n} x_j \mathbf{A}_{*j} = \mathbf{A}\mathbf{x}$$

kde $\mathbf{x} = (x_1, \ldots, x_n)^T$. Protože $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ je báze v $\mathbf{T}^n$ platí

$$\mathbf{x} = \sum_{i=1}^{k} a_i \mathbf{x}_i + \sum_{j=1}^{n} b_j \mathbf{y}_j$$

$$\mathbf{A}\mathbf{x} = \sum_{i=1}^{k} a_i \mathbf{A}\mathbf{x}_i + \sum_{j=1}^{n} b_j \mathbf{A}\mathbf{y}_j = \sum_{j=1}^{n} b_j \mathbf{A}\mathbf{y}_j \in \mathbf{S}(\mathbf{A})$$

(první suma je pouze sumou nul protože $\mathbf{x}_i \in \mathbf{N}(\mathbf{A})$).
Tedy $\mathbf{A}\mathbf{x} \in \mathbf{L}(\mathbf{A}\mathbf{y}_1, \ldots, \mathbf{A}\mathbf{y}_{n-k})$. Proto $\{\mathbf{A}\mathbf{y}_1, \ldots, \mathbf{A}\mathbf{y}_{n-k}\}$ generuje $\mathbf{S}(\mathbf{A})$.
2. je lineárně nezávislá: Nechť

$$\sum_{j=1}^{n-k} b_j \mathbf{A}\mathbf{y}_j = \mathbf{0}$$

$$\mathbf{A}\left(\sum_{j=1}^{n-k} b_j \mathbf{y}_j\right) = \mathbf{0}$$

Tedy

$$\mathbf{w} = \sum_{j=1}^{n} b_j \mathbf{y}_j \in \mathbf{N}(\mathbf{A})$$

Proto

$$\sum_{i=1}^{k} a_i \mathbf{x}_i + \sum_{j=1}^{n-k} (-b_j)\mathbf{y}_j = \mathbf{0}$$

Protože $\{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}_1, \ldots, \mathbf{y}_{n-k}\}$ je lineárně nezávislá, platí: $a_1 = \cdots = a_k = 0 = b_1 = \cdots = b_{n-k} \Rightarrow \{\mathbf{A}\mathbf{y}_1, \ldots, \mathbf{A}\mathbf{y}_{n-k}\}$ je lineárně nezávislá.
$\{\mathbf{A}\mathbf{y}_1, \ldots, \mathbf{A}\mathbf{y}_{n-k}\}$ je tedy báze $\mathbf{S}(\mathbf{A})$, z toho vyplývá, že $\dim \mathbf{S}(\mathbf{A}) = r(\mathbf{A}) = n - k = n - \dim \mathbf{N}(\mathbf{A}) \Leftrightarrow \dim \mathbf{N}(\mathbf{A}) + r(\mathbf{A}) = n$. □

Věta 4.23 *Předpokládáme, že* $\mathbf{A}$ *je matice typu* $m \times n$. *Pak platí*

1. $\dim \mathbf{S}(\mathbf{A}) = r(\mathbf{A})$,
2. $\dim \mathbf{N}(\mathbf{A}) = n - r(\mathbf{A})$,
3. $\dim \mathbf{R}(\mathbf{A}) = \dim \mathbf{S}(\mathbf{A}^T) = r(\mathbf{A})$,
4. $\dim \mathbf{N}(\mathbf{A}^T) = m - r(\mathbf{A})$.

Důkaz.
1. Z definice $r(\mathbf{A})$.
2. Plyne ihned z Věty **??**.
3. Z Důsledku **??** víme, že $r(\mathbf{A}) = r(\mathbf{A}^T)$, z definice hodnosti matice máme $r(\mathbf{A}^T) = \dim \mathbf{S}(\mathbf{A}^T)$, z Věty **??** víme, že $\dim \mathbf{S}(\mathbf{A}) = \dim \mathbf{R}(\mathbf{A})$.

Tedy $\dim \mathbf{R}(\mathbf{A}) = \dim \mathbf{S}(\mathbf{A}) = r(\mathbf{A}) = r(\mathbf{A}^T) = \dim \mathbf{S}(\mathbf{A}^T)$.
4. Je-li $\mathbf{B} = \mathbf{A}^T$ matice typu $n \times m$, pak podle Věty **??** platí, že $\dim \mathbf{N}(\mathbf{B}) + r(\mathbf{B}) = m$, tedy $\dim(\mathbf{A}^T) + r(\mathbf{A}^T) = m$, podle Důsledku **??** navíc platí, že $r(\mathbf{A}) = r(\mathbf{A}^T)$. Tedy $\dim \mathbf{N}(\mathbf{A}^T) + r(\mathbf{A}^T) = \dim \mathbf{N}(\mathbf{A}^T) + r(\mathbf{A}) = m \Leftrightarrow \dim \mathbf{N}(\mathbf{A}^T) = m - r(\mathbf{A})$. □

Věta 4.24 ***Frobeniova věta*** *Soustava lineárních rovnic* $\mathbf{Ax} = \mathbf{b}$ *je řešitelná právě když*

$$r(\mathbf{A}) = r(\mathbf{A}|\mathbf{b}).$$

Důkaz. Platí $\mathbf{S}(\mathbf{A}) \subseteq \mathbf{S}(\mathbf{A}|\mathbf{b})$. Rovnost $\mathbf{S}(\mathbf{A}) = \mathbf{S}(\mathbf{A}|\mathbf{b})$ nastává právě když $\mathbf{b} \in \mathbf{L}(\mathbf{A}_{*1}, \ldots, \mathbf{A}_{*n})$, což je právě tehdy, když existuje $\mathbf{x} = (x_1, \ldots, x_n)^T$ takový, že

$$\mathbf{b} = \sum_{i=1}^{n} x_i \mathbf{A}_{*i} \Leftrightarrow \mathbf{b} = \mathbf{Ax} \Leftrightarrow \cdots$$

$\cdots \Leftrightarrow \mathbf{Ax} = \mathbf{b}$ je řešitelná.
Rovnost $r(\mathbf{A}) = r(\mathbf{A}|\mathbf{b})$ platí $\Leftrightarrow \mathbf{S}(\mathbf{A}) = \mathbf{S}(\mathbf{A}|\mathbf{b}) \Leftrightarrow \mathbf{Ax} = \mathbf{b}$ je řešitelná. □

Příklad 4.2 Vzorec pro n-tý prvek Fibonacciovy posloupnosti.

Kapitola 5

Permutace

Definice 5.1 *Vzájemně jednoznačné zobrazení $p : X \to X$ nazýváme* permutace *na množině X. Je-li p permutace na množině X, pak inverzní zobrazení $p^{-1} : X \to X$ nazýváme* inverzní permutace *k permutaci p. Jsou-li p, q dvě permutace na množině X, pak složené zobrazení, tj. permutaci, $q \circ p : X \to X$, která prvku $x \in X$ přiřazuje prvek $q(p(x))$ nazýváme* složení permutací *p a q (v tomto pořadí). Identické zobrazení $\imath : X \to X$, pro které platí $\imath(x) = x$ pro každé $x \in X$, nazýváme* identická permutace *na množině X.*

Lemma 5.1 *Pro skládání permutací na množině X platí:*

1. *$p \circ \imath = \imath \circ p = p$ pro každou permutaci p na množině X,*
2. *$p \circ p^{-1} = p^{-1} \circ p = \imath$ pro každou permutaci p na množině X,*
3. *$r \circ (q \circ p) = (r \circ q) \circ p$ pro každé tři permutace p, q, r na množině X.*

Budeme se zabývat výhradně permutacemi na množině $\{1, 2, \ldots, n\}$. Množinu všech permutací na $\{1, 2, \ldots, n\}$ budeme nazývat *grupa všech permutací* na množině $\{1, 2, \ldots, n\}$ a budeme ji označovat S_n.

Permutace můžeme zapisovat různým způsobem. V případě permutací na konečné množině $X = \{1, 2, \ldots, n\}$ je můžeme zapsat pomocí tabulky. Do tabulky napíšeme do horního řádku čísla $1, 2, \ldots, n$ a pod každé číslo i napíšeme hodnotu $p(i)$. Tak například

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

je permutace na množině $\{1, 2, \ldots, 9\}$. Na pořadí prvků v horním řádku nezáleží, zápis

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

Pokud se domluvíme, že v horním řádku budeme psát čísla vždy ve stejném pořadí $1, 2, \ldots, n$, tak stačí zapsat pouze druhý řádek této tabulky $(3, 5, 2, 9, 4, 1, 8, 7, 6)$. Ne vždy je ale taková domluva vhodná.

Permutace můžeme zapisovat rovněž graficky. V rovině si zvolíme body $1, 2, \ldots, n$, a pokud permutace p zobrazuje prvek i do prvku $j = p(i)$, pak nakreslíme šipku z bodu i do bodu $j = p(i)$. Takovému obrázku říkáme *graf permutace* p. Graf permutace je charakterizován vlastnostmi

- z každého bodu $i \in \{1, 2, \ldots, n\}$ vychází právě jedna šipka, neboť hodnota $p(i)$ je určena jednoznačně pro každý bod $i \in \{1, 2, \ldots, n\}$,
- do každého bodu $j \in \{1, 2, \ldots, n\}$ vede právě jedna šipka, neboť pro každý bod $j \in \{1, 2, \ldots, n\}$ existuje právě jeden bod $i \in \{1, 2, \ldots, n\}$ takový, že $j = p(i)$.

Z grafu permutace je ihned vidět, že každá permutace se skládá z několika cyklů. Tak například uvedená permutace p na množině $\{1, 2, \ldots, 9\}$ se skládá ze dvou cyklů. Jeden je na bodech $1, 3, 2, 5, 4, 9, 6$, má délku 7, a druhý je na bodech $7, 8$, má délku 2. Permutaci tak můžeme zapsat v *cyklickém zápisu* jako

$$p = (1, 3, 2, 5, 4, 9, 6), (7, 8).$$

Každý bod z množiny $\{1, 2, \ldots, 9\}$ se zobrazí do bodu, který v zápisu následuje těsně za ním ve stejné závorce. Poslední bod v nějaké závorce se zobrazí do prvního bodu v téže závorce.

Pro obecnou permutaci p na nějaké konečné množině X najdeme cyklus obsahující bod $i_1 \in X$ tak, že postupně zapisujeme, kam se permutací p zobrazuje. Proto $i_2 = p(i_1)$, $i_3 = p(i_2)$, ..., tj. $i_{k+1} = p(i_k)$ pro libovolné $k > 0$. Protože je množina X konečná, musí se v posloupnosti $i_1, i_2, \ldots$ nějaký prvek opakovat. Označme $k + 1$ nejmenší index takový, že i_{k+1} se rovná některému z předcházejících prvků posloupnosti $i_1, \ldots, i_k$. To znamená, že $p(i_k) = i_{k+1} \in \{i_1, \ldots, i_k\}$. To znamená, že $p(i_k) = i_j$ pro nějaké $j \leq k$. Pokud by bylo $j > 1$, platilo by $p(i_k) = p(i_{j-1}) = p_j$. Protože i_{k+1} byl první prvek posloupnosti $i_1, i_2, \ldots$, který se rovnal některému z předchozích prvků, bylo by $i_k \neq i_{j-1}$, což je ve sporu se vzájemnou jednoznačností permutace p. Proto $j = 1$, tj. $p(i_k) = i_1$. Cyklus permutace p obsahující bod i_1 se proto rovná $(i_1, i_2, \ldots, i_k)$. Počet jeho prvků, tj. číslo k, se nazývá *délka* tohoto

cyklu. Je také dobré uvědomit si, že permutace $p \in S_n$ se rovná identické permutaci $\imath$ právě když má všechny cykly délky 1.

Cyklický zápis rovněž popisuje permutaci p jednoznačně stejně jako tabulka nebo graf. Pokud jsou v permutaci nějaké cykly délky 1, tak je obvykle v cyklickém zápisu vynecháváme. V tom případě mluvíme o *redukovaném cyklickém zápisu* permutace. Tak například cyklický zápis permutace

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

se rovná

$$q = (1), (2), (3, 4, 5, 6, 7, 8), (9)$$

a redukovaný cyklický zápis téže permutace q je

$$q = (3, 4, 5, 6, 7, 8).$$

V případě redukovaného cyklického zápisu musíme být předem domluveni, na jaké množině je permutace q definovaná.

Skládání permutací

Nejdříve si ukážeme, jak najít tabulku složené permutace $q \circ p$, známe-li tabulky permutací p a q. Vezmeme například výše uvedené permutace p, q. Uděláme si tabulku o třech řádcích tak, že horní dva řádky budou tvořit tabulku permutace p a dolní dva řádky tabulku permutace q. Dostaneme tak

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

V každém sloupci máme pod prvkem i ve druhém řádku prvek $p(i)$ a ve třetím řádku prvek $q(p(i))$. Tabulku složené permutace $q \circ p$ nyní dostaneme tak, že vynecháme druhý řádek:

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

Také graf složení dvou permutací snadno získáme z grafů obou permutací. Pro obě permutace použijeme stejnou množinu bodů v rovině. Máme-li najít graf složené permutace $q \circ p$ najdeme napřed šipku v grafu p, která vede z bodu i do bodu $p(i)$ a potom navážeme šipkou v grafu permutace q, která vede z bodu $p(i)$ do bodu $q(p(i))$. V grafu složené permutace $q \circ p$ pak vede šipka z bodu i do bodu $q \circ p(i) = q(p(i))$.

O něco složitější je najít cyklický zápis a redukovaný cyklický zápis složené permutace $q \circ p$, známe-li odpovídající zápisy permutací p a q. Pro různé otázky o permutacích je třeba zvolit vždy ten zápis, který je pro řešení příslušné úlohy nejvhodnější.

Definice 5.2 *Permutace $t \in S_n$ se nazývá* transpozice, *pokud má jeden cyklus délky* 2 *a ostatní cykly délky* 1.

Pro zápis transpozic používáme nejčastěji redukovaný cyklický zápis $t = (i, j)$.

Lemma 5.2 *Každou permutaci $p \in S_n$, kde $n \geq 2$, lze vyjádřit jako složení transpozic.*

Důkaz. Budeme předpokládat, že $p \neq \imath$. V permutaci p tak existuje aspoň jeden cyklus délky aspoň 2. Označíme si jej $(i_1, i_2, \ldots, i_k)$. Složíme permutaci p s transpozicí (i_1, i_2). Dostaneme tak permutaci $(i_1, i_2) \circ p$. V této složené permutaci se cyklus $(i_1, i_2, \ldots, i_k)$ rozpadne na dva cykly (i_1) a $(i_2, \ldots, i_k)$, a všechny ostatní cykly zůstanou beze změny.

V permutaci $(i_2, i_3) \circ (i_1, i_2) \circ p$ se tak původní cyklus $(i_1, i_2, \ldots, i_k)$ rozpadne do tří cyklů (i_1), (i_2) a $(i_3, \ldots, i_k)$. Jednoduchou indukcí podle k tak dokážeme, že v permutaci

$$(i_{k-1}, i_k) \circ (i_{k-2}, i_{k-1}) \circ \cdots \circ (i_1, i_2) \circ p$$

se původní cyklus $(i_1, i_2, \ldots, i_k)$ rozpadne na k cyklů délky 1 a všechny ostatní cykly permutace p zůstanou beze změny.

Opakujeme-li celý postup s dalším cyklem $(j_1, \ldots, j_l)$, dostaneme permutaci

$$(j_{l-1}, j_l) \circ (j_{l-2}, j_{l-1}) \circ \cdots \circ (j_1, j_2) \circ (i_{k-1}, i_k) \circ (i_{k_2}, i_{k-1}) \circ \cdots \circ (i_1, i_2) \circ p,$$

ve které se dva cykly $(i_1, i_2, \ldots, i_k)$ a $(j_1, \ldots, j_l)$ původní permutace p rozpadnou na cykly délky 1 a všechny ostatní cykly zůstávají beze změny. Postupně rozkládáme tímto způsobem další cykly permutace p na cykly délky 1, dokud nedostaneme identickou permutaci $\imath$. Existují proto transpozice $t_1, \ldots, t_m$, pro které platí

$$t_m \circ \cdots \circ t_1 \circ p = \imath.$$

Protože pro každou transpozici t platí $t = t^{-1}$, tj. $t \circ t = \imath$, můžeme poslední rovnost složit z transpozicí t_m zleva a dostaneme tak

$$t_{m-1} \circ \ldots \circ t_1 \circ p = t_m.$$

Postupným skládáním s transpozicemi $t_{m-1}, \ldots, t_1$ zleva tak dostaneme rovnost

$$p = t_1 \circ t_2 \circ \cdots \circ t_m,$$

což znamená, že jsme permutaci p vyjádřili jako složení transpozic. V případě identické permutace stačí vzít vyjádření $\imath = t \circ t$ pro libovolnou transpozici $t \in S_n$. □

Lemma 5.3 *Počet cyklů v permutaci $p \in S_n$ a permutaci $t \circ p$, kde $t \in S_n$ je libovolná transpozice, se liší o 1. Rovněž počty cyklů v permutacích p a $p \circ t$ se liší o 1.*

Důkaz. Označíme $t = (i, j)$. Napřed budeme předpokládat, že prvky i, j leží ve stejném cyklu $(i_1, \ldots, i_k, j_1, \ldots, j_l)$ permutace p a $i = i_1$, $j = j_1$. Pak platí, že v permutaci $t \circ p$ se tento cyklus rozpadne na dva cykly $(i_1, \ldots, i_k)$ a $(j_1, \ldots, j_l)$ a ostatní cykly zůstanou beze změny. Počet cyklů v permutaci $t \circ p$ je tak o 1 větší, než počet cyklů v permutaci p.

Jsou-li prvky i, j z různých cyklů $(i = i_1, \ldots, i_k)$ a $(j = j_1, \ldots, j_l)$ permutace p, potom ve složení $t \circ p$ se oba cykly propojí do jednoho cyklu $(i_1, \ldots, i_k, j_1, \ldots, j_l)$ a ostatní cykly zůstanou beze změny, počet cyklů v permutaci $t \circ p$ je proto o 1 menší než počet cyklů v permutaci p.

Zcela stejně dokážeme, že také počet cyklů v permutaci $p \circ t$ se liší o 1 od počti cyklů v permutaci p. □

Lemma 5.4 *Jsou-li $p = t_1 \circ \cdots \circ t_k$ a $p = u_1 \circ \cdots \circ u_l$ dvě různá vyjádření permutace $p \in S_n$ jako složení transpozic, pak jsou obě čísla k, l buď současně sudá nebo jsou současně lichá.*

Důkaz. Z rovnosti $t_1 \circ \cdots \circ t_k = u_1 \circ \cdots \circ u_l$ dostaneme postupným skládáním s transpozicemi $t_1, \ldots, t_k$ zleva rovnost

$$t_k \circ \cdots \circ t_1 \circ u_1 \circ \cdots \circ u_l = \imath.$$

To znamená, že počet cyklů v obou permutacích $\imath$ a $t_k \circ \cdots \circ t_1 \circ u_1 \circ \cdots \circ u_l$ je stejný a rovná se n. Podle předchozího Tvrzení **??** se počet cyklů v jakékoliv permutaci změní o 1, pokud ji složíme s transpozicí. Proto musí být počet transpozic $k + l$ ve složení $t_k \circ \cdots \circ t_1 \circ u_1 \circ \cdots \circ u_l$ sudý, a tedy jsou čísla k, l buď obě sudá nebo obě lichá. □

Definice 5.3 *Permutace $p \in S_n$ se nazývá* sudá, *pokud ji lze vyjádřit jako složení sudého počtu transpozic. Nazývá se* lichá, *pokud ji lze vyjádřit jako*

složení lichého počtu transpozic. Definujeme také znaménko permutace p *jako* 1, *pokud je* p *sudá permutace, a jako* -1, *pokud je* p *lichá permutace. Znaménko permutace* p *označujeme jako* $\operatorname{sgn} p$.

Tvrzení 5.5 *Složení dvou sudých permutací nebo dvou lichých permutací je sudá permutace. Složení sudé permutace s lichou (v jakémkoliv pořadí) je lichá permutace. Speciálně, pro každou permutaci* $p \in S_n$ *a každou transpozici* $t \in S_n$ *platí*

$$\operatorname{sgn}(t \circ p) = \operatorname{sgn}(p \circ t) = -\operatorname{sgn} p.$$

Důkaz. Plyne okamžitě z předchozího Tvrzení **??**. Pokud $p = t_1 \circ \cdots \circ t_k$ a $q = u_1 \circ \cdots \circ u_l$, pak $q \circ p = (u_1 \circ \cdots \circ u_l) \circ (t_1 \circ \cdots \circ t_k)$, permutaci $q \circ p$ proto dostaneme jako složení $k + l$ transpozic. □

Lemma 5.6 *Je-li* k *počet cyklů permutace* $p \in S_n$, *pak* $\operatorname{sgn} p = (-1)^{n-k}$.

Důkaz. Permutaci p vyjádříme jako složení transpozic $p = (t_1 \circ \cdots \circ t_l) \circ \imath$. Přidáním indentické permutace $\imath$ se složení nezmění. Identická permutace $\imath$ má n cyklů, zatímco permutace p má k cyklů. To znamená, že číslo l musí mít stejnou paritu jako číslo $n - k$ (to znamená, že obě čísla musí být současně sudá nebo současně lichá). Z Definice **??** tak plyne

$$\operatorname{sgn} p = (-1)^l = (-1)^{n-k}.$$

□

Úloha 5.1 Dokažte, že permutace $p \in S_n$ je sudá právě když má sudý počet cyklů sudé délky a je lichá právě když má lichý počet cyklů sudé délky.

Příklad 5.1 Charakterizace řešitelných a neřešitelných pozic u hry "15".

Kapitola 6

Determinanty

Definice 6.1 *Je-li* $\mathbf{A} = (a_{ij})$ *čtvercová matice řádu* n *s prvky z tělesa* $\mathbf{T}$, *pak definujeme* determinant *matice* $\mathbf{A}$ *jako číslo*

$$\det \mathbf{A} = \sum_{p \in S_n} \operatorname{sgn} p \cdot a_{1p(1)} a_{2p(2)} \cdots a_{np(n)} \in \mathbf{T}.$$

Determinant matice $\mathbf{A}$ *označujeme rovněž* $|\mathbf{A}|$.

Pro zjednodušení zápisu budeme nadále v definici determinantu používat označení $p_i = p(i)$ pro $i = 1, 2, \ldots, n$ a $p \in S_n$.

Příklad 6.1 Vypočtěte determinanty matic druhého a třetího řádu.

Lemma 6.1 *Je-li* $\mathbf{A} = (a_{ij})$ *horní trojúhelníková matice, pak* $\det \mathbf{A} = a_{11} a_{22} \cdots a_{nn}$.

Důkaz. Matice $\mathbf{A}$ je horní trojúhelníková právě když $a_{ij} = 0$ kdykoliv $i > j$. Dokážeme, že pro jakoukoliv permutaci $p \neq \imath$ je součin $a_{1p_1} a_{2p_2} \cdots a_{np_n} = 0$. Protože předpokládáme, že p je neindentická permutace, existuje $j \in \{1, 2, \ldots, n\}$ takové, že $p(j) \neq j$. Je-li $p(j) < j$, je prvek $a_{jp_j} = 0$ a tedy celý součin $a_{1p_1} a_{2p_2} \cdots a_{np_n} = 0$. Pokud $p(j) > j$, označíme k délku cyklu obsahující prvky $j, p(j)$. Tento cyklus se pak rovná $(j, p(j), p^2(j), \ldots, p^{k-1}(j))$. Je-li tato posloupnost rostoucí, platí $j < p^{k-1}(j)$. Označíme $i = p^{k-1}(j)$. Potom $p(i) = j < i$ a prvek $a_{ip_i} = 0$. V opačném případě existuje $l < k - 1$ takové, že $p^l(j) > p^{l+1}(j)$. Opět označíme $i = p^l(j)$ a dostaneme, že $i > p(i)$. I v tomto případě je tak $a_{1p_1} a_{2p_2} \cdots a_{np_n} = 0$.

V součtu definujícím determinant tak můžeme vynechat všechny sčítance pro neindentické permutace. Zbývá jediný sčítanec pro $p = \imath$, který se rovná $a_{11}a_{22}\cdots a_{nn}$. A protože identická permutace je sudá, je tento sčítanec se znaménkem $+$. □

Příklad 6.2 Geometrický význam determinantů matic druhého a třetího řádu.

Tvrzení 6.2 *Pro každou čtvercovou matici* $\mathbf{A} = (a_{ij})$ *řádu* n *platí*

$$\det \mathbf{A} = \det \mathbf{A}^T.$$

Důkaz. Označme si transponovanou matici $\mathbf{A}^T = \mathbf{B} = (b_{ij})$. Pro libovolnou permutaci $p = (p_1, p_2 \ldots, p_n) \in S_n$ (zápis tabulkou) je součin $a_{1p_1}a_{1p_2}\cdots a_{np_n} = b_{p_1 1}b_{p_2 2}\cdots b_{p_n n}$. Součin $a_{1p_1}a_{1p_2}\cdots a_{np_n}$ se při výpočtu $\det \mathbf{A}$ vyskytuje se znaménkem $\operatorname{sgn} p$, zatímco tentýž součin $b_{p_1 1}b_{p_2 2}\cdots b_{p_n n}$ odpovídá při výpočtu $\det \mathbf{B}$ permutaci p^{-1} a má tedy znaménko $\operatorname{sgn} p^{-1} = \operatorname{sgn} p$. V součtech definujících $\det \mathbf{A}$ a $\det \mathbf{B}$ se tak vyskytují stejné součiny se stejným znaménkem, proto $\det \mathbf{A} = \det \mathbf{B} = \det \mathbf{A}^T$. □

Tvrzení 6.3 *Má-li matice* $\mathbf{A}$ *řádu* n *dva stejné řádky, pak* $\det \mathbf{A} = 0$.

Důkaz. Předpokládáme, že $\mathbf{A}_{i*} = \mathbf{A}_{j*}$ pro $i < j$, tj. $a_{ik} = a_{jk}$ pro $k = 1, 2, \ldots, n$. Označme $t = (i, j)$ transpozici, která prohazuje i-tý a j-tý řádek. Zvolíme libovolnou permutaci $p \in S_n$ a podíváme se, jaké součiny v součtu definujícím $\det \mathbf{A}$ určují permutace p a $q = p \circ (i, j) = p \circ t$. Platí $q(i) = p(j)$, $q(j) = p(i)$ a $q(k) = p(k)$ pro $k \neq i, j$. Permutace p určuje součin

$$\operatorname{sgn} p \cdot a_{1p_1} \cdots a_{ip_i} \cdots a_{jp_j} \cdots a_{np_n},$$

zatímco permutace $q = p \circ t$ určuje součin

$$\begin{aligned} & \operatorname{sgn} q \cdot a_{1q_1} \cdots a_{iq_i} \cdots a_{jq_j} \cdots a_{nq_n} = \\ = \; & \operatorname{sgn} (p \circ t) \cdot a_{1q_1} \cdots a_{iq_i} \cdots a_{jq_j} \cdots a_{nq_n} = \\ = \; & -\operatorname{sgn} p \cdot a_{1p_1} \cdots a_{ip_j} \cdots a_{jp_i} \cdots a_{np_n} = \\ = \; & -\operatorname{sgn} p \cdot a_{1p_1} \cdots a_{ip_i} \cdots a_{jp_j} \cdots a_{np_n}. \end{aligned}$$

Je $q = p \circ t \neq p$ neboť jedna z permutací p, q je sudá a druhá lichá podle Tvrzení **??**. Součet součinů určených permutacemi p, q se tak rovná

$$\operatorname{sgn} p \cdot a_{1p_1} \cdots a_{ip_i} \cdots a_{jp_j} \cdots a_{np_n} + \operatorname{sgn} q \cdot a_{1q_1} \cdots a_{iq_i} \cdots a_{jq_j} \cdots a_{nq_n} = 0.$$

Celou množinu indexů, tj. symetrickou grupu S_n, rozložíme do disjunktních dvojic permutací $\{p, p \circ t\}$. Tyto dvojice jsou skutečně disjunktní. Z rovnosti permutací $p = r$ plyne rovnost $p \circ t = r \circ t$. Podobně z rovnosti $p \circ t = r \circ t$ vyplývá $p = (p \circ t) \circ t = (r \circ t) \circ t = r$ a rovnost $p = r \circ t$ platí právě když $p \circ t = (r \circ t) \circ t = r$. Pokud se tedy dvě dvojice $\{p, p \circ t\}$ a $\{r, r \circ t\}$ protínají, musí se rovnat. Celý součet

$$\sum_{p \in S_n} \operatorname{sgn} p \cdot a_{1p_1} a_{2p_2} \cdots a_{np_n} \in \mathbf{T}.$$

definující $\det \mathbf{A}$ tak můžeme rozložit do neprotínajících se dvojic, z nichž součet každé dvojice se rovná 0. Proto také

$$\det \mathbf{A} = \sum_{p \in S_n} \operatorname{sgn} p \cdot a_{1p_1} a_{2p_2} \cdots a_{np_n} \in \mathbf{T} = 0.$$

□

Věta 6.4 *Předpokládáme, že $\mathbf{A} = (a_{ij})$ je čtvercová matice řádu n a $\mathbf{B} = (b_{ij})$ je matice, kterou dostaneme z matice $\mathbf{A}$ nějakou elementární řádkovou úpravou, pak*

- $\det \mathbf{B} = -\det \mathbf{A}$*, pokud jsme* $\mathbf{B}$ *dostali z* $\mathbf{A}$ *prohozením dvou řádků,*
- $\det \mathbf{B} = c \cdot \det \mathbf{A}$*, pokud jsme* $\mathbf{B}$ *dostali z* $\mathbf{A}$ *vynásobením některého řádku prvkem* $0 \neq c \in \mathbf{T}$*,*
- $\det \mathbf{B} = \det \mathbf{A}$*, pokud jsme dostali* $\mathbf{B}$ *z* $\mathbf{A}$ *pomocí třetí elementární řádkové úpravy.*

Důkaz. V případě první elementární úpravy platí $\mathbf{B}_{i*} = \mathbf{A}_{j*}$ a $\mathbf{B}_{j*} = \mathbf{A}_{j*}$ pro nějaké indexy $i < j$, a $\mathbf{B}_{k*} = \mathbf{A}_{k*}$ pro $k \neq i, j$. Porovnáme součin určený nějakou permutací $p \in S_n$ v součtu definujícím $\det \mathbf{A}$ a součin určený permutací $q = p \circ t$ v součtu definujícím $\det \mathbf{B}$. Stejně jako v důkazu předchozího tvrzení označuje t transpozici (i, j). Platí

$$\begin{aligned}\operatorname{sgn} q \cdot b_{1q_1} \cdots b_{iq_i} \cdots b_{jq_j} \cdots b_{nq_n} &= \operatorname{sgn}(p \circ t) \cdot a_{1p_1} \cdots a_{jp_j} \cdots a_{ip_i} \cdots a_{np_n} = \\ &= -\operatorname{sgn} p \cdot a_{1p_1} \cdots a_{ip_i} \cdots a_{jp_j} \cdots a_{np_n}.\end{aligned}$$

V součtech definujících $\det \mathbf{B}$ a $\det \mathbf{A}$ se tak vyskytují stejné součiny, ale s opačnými znaménky. Proto $\det \mathbf{B} = -\det \mathbf{A}$.

Pro důkaz druhého tvrzení si připomeňme, že v matici $\mathbf{B}$ platí $\mathbf{B}_{i*} = c\mathbf{A}_{i*}$ pro nějaké $i \in \{1, 2, \ldots, n\}$, a $\mathbf{B}_{k*} = \mathbf{A}_{k*}$ pro $k \neq i$. Platí proto

$b_{ij} = ca_{ij}$ a $b_{kj} = a_{kj}$ pro libovolné j a $k \neq i$. Permutace $p \in S_n$ tak určuje v součtu definujícím $\det \mathbf{B}$ součin

$$\begin{aligned} & \operatorname{sgn} p \cdot b_{1p_1} b_{2p_2} \cdots b_{ip_i} \cdots b_{np_n} = \operatorname{sgn} p \cdot a_{1p_1} a_{2p_2} \cdots ca_{ip_i} \cdots a_{np_n} = \\ = \; & c \cdot \operatorname{sgn} p \cdot a_{1p_1} a_{2p_2} \cdots a_{ip_i} \cdots a_{np_n}. \end{aligned}$$

Součin určený permutací p v definici $\det \mathbf{B}$ tak dostaneme ze součinu určeného stejnou permutací p v definici $\det \mathbf{A}$ vynásobením skalárem c. Protože to platí pro každou permutaci $p \in S_n$, dostáváme rovnost $\det \mathbf{B} = c \cdot \det \mathbf{A}$.

Konečně třetí elementární úpravou k i-tému řádku matice $\mathbf{A}$ přičítáme c-násobek j-tého řádku. Budeme opět předpokládat $i < j$, případ $i > j$ se dokáže zcela stejně. V tomto případě máme $b_{ik} = a_{ik} + ca_{jk}$ pro každé $k = 1, 2, \ldots, n$. Dále $b_{lk} = a_{lk}$ pro každé $l \neq i$ a $k \in \{1, 2, \ldots, n\}$. Permutace $p \in S_n$ určuje v definici $\det \mathbf{B}$ součin

$$\begin{aligned} & b_{1p_1} \cdots b_{ip_i} \cdots b_{jp_j} \cdots b_{np_n} = a_{1p_1} \cdots (a_{ip_i} + ca_{jp_i}) \cdots a_{jp_j} \cdots a_{np_n} = \\ = \; & a_{1p_1} \cdots a_{ip_i} \cdots a_{jp_j} \cdots a_{np_n} + a_{1p_1} \cdots (ca_{jp_i}) \cdots a_{jp_j} \cdots a_{np_n} = \\ = \; & a_{1p_1} \cdots a_{ip_i} \cdots a_{jp_j} \cdots a_{np_n} + c \cdot a_{1p_1} \cdots a_{jp_i} \cdots a_{jp_j} \cdots a_{np_n}. \end{aligned}$$

První sčítanec v závěrečném součtu se rovná součinu určenému permutací p v $\det \mathbf{A}$, zatímco druhý sčítanec se rovná c-násobku součinu určeného permutací p v determinantu matice, jejíž i-tý řádek se rovná j-tému řádku. Taková matice má determinant rovný 0 podle Tvrzení **??**. Proto

$$\det \mathbf{B} = \sum_{p \in S_n} \operatorname{sgn} p \cdot b_{1p_1} \cdots b_{np_n} = \sum_{p \in S_n} \operatorname{sgn} p \cdot a_{1p_1} \cdots a_{np_n} = \det \mathbf{A}.$$

□

Všimněte si, že v případě, kdy charakteristika tělesa $\mathbf{T}$ je různá od 2, plyne Tvrzení **??** z první části Věty **??**. Jsou-li v matici $\mathbf{A}$ dva řádky – i-tý a j-tý – stejné, pak prohozením těchto dvou řádků dostaneme matici $\mathbf{B} = \mathbf{A}$. Podle první části Věty **??** platí $\det \mathbf{A} = \det \mathbf{B} = -\det \mathbf{A}$, tj. $\det \mathbf{A} + \det \mathbf{A} = 0$. Protože má těleso $\mathbf{T}$ charakteristiku různou od 2, plyne odtud $\det \mathbf{A} = 0$. Pouze v případě, kdy má těleso $\mathbf{T}$ charakteristiku rovnou 2, z rovnosti $\det \mathbf{A} + \det \mathbf{A} = 0$ nevyplývá $\det \mathbf{A} = 0$. V takovém případě je nutné použít Tvrzení **??**.

Důsledek 6.5 *Pro determinanty elementárních matic řádu n platí*

- $\det \mathbf{E}_{ij} = -1$,
- $\det \mathbf{E}_i(c) = c$,

- $\det \mathbf{E}_{ij}(d) = 1$.

Pro každou elementární matici $\mathbf{E}$ *a libovolnou matici* $\mathbf{A}$ *téhož řádu* n *platí*

$$\det \mathbf{EB} = \det \mathbf{E} \cdot \det \mathbf{B}.$$

Důkaz. Každou elementární matici dostaneme z jednotkové matice $\mathbf{I}$ odpovídající elementární řádkovou úpravou. Protože $\det \mathbf{I} = 1$ neboť jednotková matice je horní trojúhelníková, plynou dodnoty determinantů všech elementárních matic z Věty **??**.

Odtud rovněž plyne druhá část důsledku za využití Věty **??**. □

Věta 6.6 *Čtvercová matice* $\mathbf{A}$ *je regulární právě když* $\det \mathbf{A} \neq 0$.

Důkaz. Podle Důsledku **??** platí rovnost

$$\det(\mathbf{EB}) = \det \mathbf{E} \cdot \det \mathbf{B}$$

pro každou elementární matici $\mathbf{E}$ a čtvercovou matici $\mathbf{B}$ stejného řádu n. Matici $\mathbf{A}$ převedeme Gaussovou eliminací pomocí elementárních řádkových úprav do matice $\mathbf{D}$ v řádkově odstupňovaném tvaru. To znamená, že existují elementární matice $\mathbf{E}_1, \mathbf{E}_2, \ldots, \mathbf{E}_k$, pro které platí $\mathbf{D} = \mathbf{E}_k \cdots \mathbf{E}_1 \mathbf{A}$. S využitím předchozí rovnosti dostáváme

$$\begin{aligned} \det \mathbf{D} = \det(\mathbf{E}_k \cdots \mathbf{E}_1 \mathbf{A}) &= \det \mathbf{E}_k \cdot \det(\mathbf{E}_{k-1} \cdots \mathbf{E}_1 \mathbf{A}) = \\ &= \det \mathbf{E}_k \cdot \det \mathbf{E}_{k-1} \cdot \det(\mathbf{E}_{k-2} \cdots \mathbf{E}_1 \mathbf{A}) = \\ &\vdots \\ &= \det \mathbf{E}_k \cdot \det \mathbf{E}_{k-1} \cdots \det \mathbf{E}_1 \cdot \det \mathbf{A}. \end{aligned}$$

Determinanty elementárních matic jsou nenulové podle Důsledku **??**, platí proto

$$\det \mathbf{A} \neq 0 \quad \text{právě když} \quad \det \mathbf{D} \neq 0.$$

Podle Věty 3.9 je matice $\mathbf{A}$ regulární právě když $\mathbf{D}$ neobsahuje žádný nulový řádek, což je právě když $\det \mathbf{D} \neq 0$, neboť matice $\mathbf{D}$ je horní trojúhelníková matice, a to je podle právě dokázané ekvivalence právě když $\det \mathbf{A} \neq 0$. □

Pomocí předchozí věty snadno dokážeme následující důležitou *větu o součinu determinantů.*

Věta 6.7 *Pro každé dvě čtvercové matice* $\mathbf{A}, \mathbf{B}$ *řádu* n *platí*

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

Důkaz. Je-li matice $\mathbf{A}$ singulární, platí $r(\mathbf{A}) < n$, a proto také podle Důsledku 6.20 $r(\mathbf{AB}) \leq r(\mathbf{A}) < n$, součin $\mathbf{AB}$ je proto také singulární matice. Z rovnosti $\det \mathbf{A} = 0$ tak plyne $\det(\mathbf{AB}) = 0$ a dokazovaná rovnost $\det(\mathbf{AB}) = \det \mathbf{A} \cdot \det \mathbf{B}$ tak platí v případě, že $\mathbf{A}$ je singulární matice.

Pokud je $\mathbf{A}$ regulární matice, můžeme ji podle podle Tvrzení 3.12 vyjádřit jako součin elementárních matic $\mathbf{A} = \mathbf{E}_k \cdots \mathbf{E}_1$. Potom platí

$$\begin{aligned} \det(\mathbf{AB}) &= \det(\mathbf{E}_k \cdots \mathbf{E}_1 \mathbf{B}) = \det \mathbf{E}_k \cdots \det \mathbf{E}_1 \cdot \det \mathbf{B} = \\ &= \det(\mathbf{E}_k \cdots \mathbf{E}_1) \cdot \det \mathbf{B} = \det \mathbf{A} \cdot \det \mathbf{B}. \end{aligned}$$

□

Nyní se budeme věnovat základní metodě výpočtu determinantů – *rozvoji determinantu podle řádku* případně *podle sloupce.*

Definice 6.2 *Je-li* $\mathbf{A} = (a_{ij})$ *čtvercová matice řádu* n*, pak pro* $i, j \in \{1, 2, \ldots, n\}$ *označujeme* $\mathbf{M}_{ij}$ *čtvercovou matici řádu* $n-1$*, kterou dostaneme z* $\mathbf{A}$ *vynecháním* i*-tého řádku a* j*-tého sloupce. Nazýváme ji* minor *matice* $\mathbf{A}$ *odpovídající místu* (i, j)*. Číslo* $m_{ij} = (-1)^{i+j} \det \mathbf{M}_{ij}$ *nazýváme* kofaktor *matice* $\mathbf{A}$ *určený místem* (i, j)*. Matici* $\mathbf{M} = (m_{ij})$ *nazýváme* kofaktorová matice *určená maticí* $\mathbf{A}$ *a transponovanou matici* $\mathbf{M}^T$ *nazýváme* adjungovaná matice *k matici* $\mathbf{A}$*. Adjungovanou matici k matici* $\mathbf{A}$ *budeme označovat* $\operatorname{adj} \mathbf{A}$*.*

Věta 6.8 *Pro každou čtvercovou matici* $\mathbf{A} = (a_{ij})$ *řádu* n *a každé* $i, j \in \{1, 2, \ldots, n\}$ *platí*

- $\det \mathbf{A} = a_{i1} m_{i1} + a_{i2} m_{i2} + \cdots + a_{in} m_{in} = \sum_{k=1}^{n} a_{ik} m_{ik}$,
- $\det \mathbf{A} = a_{1j} m_{1j} + a_{2j} m_{2j} + \cdots + a_{nj} m_{nj} = \sum_{k=1}^{n} a_{kj} m_{kj}$.

Důkaz. Dokážeme první z obou tvrzení o rozvoji determinantu podle i-tého řádku. Druhé tvrzení o rozvoji determinantu podle j-tého sloupce pak vyplyne z rozvoje podle j-tého řádku a z Tvrzení **??**.

Začneme tím, že se podíváme na všechny součiny v součtu definujícím $\det \mathbf{A}$, které obsahují činitele a_{nn}. Tyto součiny jsou určené permutacemi $p \in S_n$, pro které platí $p(n) = n$. Každý takový součin má tvar

$$\operatorname{sgn} p \cdot a_{1p_1} a_{2p_2} \cdots a_{n-1p_{n-1}} a_{nn}.$$

Součet všech těchto součinů se potom rovná

$$\sum_{p(n)=n} \operatorname{sgn} p \cdot a_{1p_1} a_{2p_2} \cdots a_{n-1p_{n-1}} a_{nn} = a_{nn} \cdot \sum_{p(n)=n} \operatorname{sgn} p \cdot a_{1p_1} a_{2p_2} \cdots a_{n-1p_{n-1}}.$$

Pokud každou permutaci $p \in S_n$, pro kterou platí $p(n) = n$, zúžíme na množinu $\{1, 2, \ldots, n-1\}$, dostaneme permutaci $q \in S_{n-1}$. Permutace q působí na množině, která má o jeden prvek méně, a sama má také o jeden cyklus méně, než permutace p. Proto $\operatorname{sgn} q = \operatorname{sgn} p$. Každou permutaci $q \in S_{n-1}$ můžeme naopak jednoznačně rozšířit do permutace $p \in S_n$ tak, že dodefinujeme $p(n) = n$. Každý člen $\operatorname{sgn} p \cdot a_{1p_1} a_{2p_2} \cdots a_{n-1p_{n-1}}$ v druhém součtu v poslední rovnosti se proto rovná $\operatorname{sgn} q \cdot a_{1q_1} a_{2q_2} \cdots a_{n-1q_{n-1}}$, kde q je zúžení permutace p na množinu $\{1, 2, \ldots, n-1\}$. Druhá suma v poslední rovnosti se proto rovná

$$\sum_{q \in S_{n-1}} \operatorname{sgn} q \cdot a_{1q_1} a_{2q_2} \cdots a_{n-1q_{n-1}} = \det \mathbf{M}_{nn},$$

součet všech součinů v $\det \mathbf{A}$ obsahujících prvek a_{nn} se tak rovná součinu $a_{nn} \cdot \det \mathbf{M}_{nn}$.

Nyní se podíváme, jak vypadají všechny součiny v $\det \mathbf{A}$ obsahující prvek a_{ij}. K tomu účelu postupně zaměníme i-tý řádek matice $\mathbf{A}$ s $(i+1)$-ním řádkem, potom s $(i+2)$-hým řádkem, atd. až s n-tým řádkem. Dostaneme tak matici, jejíž n-tý řádek se rovná i-tému řádku matice $\mathbf{A}$ a pořadí ostatních řádků se nezměnilo. Speciálně, prvek na místě (n, j) nové matice se rovná a_{ij}.

Dále pokračujeme tak, že postupně prohazujeme j-tý sloupec s $(j+1)$-ním sloupcem, pak s $(j+2)$-hým sloupcem, a tak dále až nakonec s n-tým sloupcem. Dostaneme tak nakonec matici $\mathbf{B} = (b_{ij})$, pro kterou platí $b_{nn} = a_{ij}$, a dále minor $\mathbf{N}_{nn}$ matice $\mathbf{B}$ odpovídající místu (n, n) se rovná minoru $\mathbf{M}_{ij}$ matice $\mathbf{A}$ odpovídajícímu místu (i, j). Součet všech součinů v $\det \mathbf{B}$ obsahujících prvek b_{nn} se podle předchozích dvou odstavců proto rovná $b_{nn} \cdot \det \mathbf{N}_{nn} = a_{ij} \cdot \det \mathbf{M}_{ij}$.

Matici $\mathbf{B}$ jsme dostali z matice $\mathbf{A}$ pomocí $n-i$ elementárních řádkových úprav prvního druhu a dále pomocí $n-j$ elementárních sloupcových úprav prvního druhu. Každá z těchto úprav mění znaménko $\det \mathbf{A}$ podle Věty **??** a Tvrzení **??**, platí proto

$$\det \mathbf{B} = (-1)^{2n-i-j} \det \mathbf{A} = (-1)^{i+j} \det \mathbf{A}.$$

Protože $\det \mathbf{A} = (-1)^{i+j} \det \mathbf{B}$, součet všech součinů v $\det \mathbf{A}$ obsahujících prvek a_{ij} se proto rovná součtu všech součinů v $\det \mathbf{B}$ obsahujících prvek $b_{nn} = a_{ij}$ s koeficientem $(-1)^{i+j}$. Podle předchozího odstavce se tak součet všech součinů v $\det \mathbf{A}$ obsahujících a_{ij} rovná

$$(-1)^{i+j} b_{nn} \cdot \det \mathbf{N}_{nn} = a_{ij} \cdot (-1)^{i+j} \det \mathbf{M}_{ij} = a_{ij} m_{ij},$$

kde m_{ij} je podle Definice **??** kofaktor matice $\mathbf{A}$ určený místem (i,j).

Protože v každém součinu v součtu definujícím $\det \mathbf{A}$ se vyskytuje právě jeden prvek z i-tého řádku matice $\mathbf{A}$, platí

$$\det \mathbf{A} = a_{i1}m_{i1}+a_{i2}m_{i2}+\cdots+a_{in}m_{in} = \sum_{k=1}^{n} a_{ik}m_{ik} = \sum_{k=1}^{n}(-1)^{i+k}a_{ik}\det \mathbf{M}_{ik}.$$

□

Úloha 6.1 Spočítejte determinant Vandermondovy matice a rozhodněte, kdy je Vandermondova matice regulární.

Řešení. Označíme

$$V_{t_0,t_1,\ldots,t_n} = \begin{vmatrix} 1 & t_0 & t_0^2 & \cdots & t_0^n \\ 1 & t_1 & t_1^2 & \cdots & t_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & t_n & t_n^2 & \cdots & t_n^n \end{vmatrix}$$

determinant Vandermondovy matice řádu n určené prvky $t_0, t_1, \ldots, t_n \in \mathbf{T}$. Pokud se dva z prvků $t_0, t_1, \ldots, t_n$ rovnají, má Vandermondova matice dva stejné řádky a její determinant se proto rovná 0 podle Tvrzení **??**. Budeme proto nadále předpokládat, že všechny prvky $t_0, t_1, \ldots, t_n$ jsou navzájem různé.

Napřed odečteme první řádek od všech ostatních. Determinant se podle Věty **??** nezmění, dostaneme tak

$$V_{t_0,t_1,\ldots,t_n} = \begin{vmatrix} 1 & t_0 & t_0^2 & \cdots & t_0^n \\ 0 & t_1-t_0 & t_1^2-t_0^2 & \cdots & t_1^n-t_0^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & t_n-t_0 & t_n^2-t_0^2 & \cdots & t_n^n-t_0^n \end{vmatrix}.$$

Nyní determinant rozvineme podle prvního sloupce a dostaneme vyjádření

$$V_{t_0,t_1,\ldots,t_n} = \begin{vmatrix} t_1-t_0 & t_1^2-t_0^2 & \cdots & t_1^n-t_0^n \\ t_2-t_0 & t_2^2-t_0^2 & \cdots & t_2^n-t_0^n \\ \vdots & \vdots & \ddots & \vdots \\ t_n-t_0 & t_n^2-t_0^2 & \cdots & t_n^n-t_0^n \end{vmatrix}.$$

Dále použijeme známý algebraický rozklad

$$t_i^j - t_0^j = (t_i-t_0)(t_i^{j-1}+t_i^{j-2}t_0+\cdots t_i t_0^{j-2}+t_0^{j-1}) = (t_i-t_0)c_{ij},$$

kde jsme pro jednoduchost označili

$$c_{ij} = t_i^{j-1} + t_i^{j-2}t_0 + \cdots t_i t_0^{j-2} + t_0^{j-1} = \sum_{k=0}^{j-1} t_i^k t_0^{j-1-k}.$$

Speciálně platí $c_{i1} = 1$ pro libovolné $i = 1, \ldots, n$. S použitím tohoto označení dostáváme

$$V_{t_0,t_1,\ldots,t_n} = \begin{vmatrix} (t_1 - t_0)c_{11} & (t_1 - t_0)c_{12} & \cdots & (t_1 - t_0)c_{1n} \\ (t_2 - t_0)c_{21} & (t_2 - t_0)c_{22} & \cdots & (t_2 - t_0)c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ (t_n - t_0)c_{n1} & (t_n - t_0)c_{n2} & \cdots & (t_n - t_0)c_{nn} \end{vmatrix}.$$

Z i-tého řádku můžeme vytknout $t_i - t_0$ pro každé $i = 1, \ldots, n$ a dosadit $c_{i1} = 1$, proto

$$V_{t_0,t_1,\ldots,t_n} = \prod_{i=1}^{n}(t_i - t_0) \begin{vmatrix} 1 & c_{12} & \cdots & c_{1n} \\ 1 & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & c_{n2} & \cdots & c_{nn} \end{vmatrix}.$$

Nyní $c_{i2} = t_i + t_0$ pro každé $i = 1, \ldots, n$. Pokud tedy odečteme od druhého sloupce t_0-násobek prvního sloupce, dostaneme

$$V_{t_0,t_1,\ldots,t_n} = \prod_{i=1}^{n}(t_i - t_0) \begin{vmatrix} 1 & t_1 & c_{13} & \cdots & c_{1n} \\ 1 & t_2 & c_{23} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & t_n & c_{n3} & \cdots & c_{nn} \end{vmatrix}.$$

Podobně $c_{i3} = t_i^2 - t_i t_0 + t_0^2$ pro každé $i = 1, \ldots, n$. Odečteme tedy od třetího sloupce t_0^2-násobek prvního sloupce a t_0-násobek druhého sloupce. Potom

$$V_{t_0,t_1,\ldots,t_n} = \prod_{i=1}^{n}(t_i - t_0) \begin{vmatrix} 1 & t_1 & t_1^2 & c_{14} & \cdots & c_{1n} \\ 1 & t_2 & t_2^2 & c_{24} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ 1 & t_n & t_n^2 & c_{n4} & \cdots & c_{nn} \end{vmatrix}.$$

Postupně tak dostaneme

$$V_{t_0,t_1,\ldots,t_n} = \prod_{i=1}^{n}(t_i - t_0) \cdot V_{t_1,\ldots,t_n}$$

Poslední výraz je rekurentní formule, pomocí které již vypočítáme hodnotu $V_{t_0,t_1,\ldots,t_n}$ Vandermonodova determinantu řádu $n+1$. Začneme hodnotami pro malá n.

$$V_{t_0} = 1, \qquad V_{t_0,t_1} = t_1 - t_0, \qquad V_{t_0,t_1,t_2} = (t_2 - t_0)(t_2 - t_1)(t_1 - t_0).$$

Pokud induktivně předpokládáme, že

$$V_{t_0,t_1,\ldots,t_{n-1}} = \prod_{\substack{i>j \\ i,j=0,\ldots,n-1}} (t_i - t_j),$$

potom pomocí již dokázané rekurentní formule dostaneme

$$\begin{aligned} V_{t_0,t_1,\ldots,t_n} &= \left(\prod_{i=1}^{n}(t_i - t_0)\right) V_{t_1,\ldots,t_n} = \prod_{i=1}^{n}(t_i - t_0) \prod_{\substack{i>j \\ i,j=1,\ldots,n}} (t_i - t_j) = \\ &= \prod_{\substack{i>j \\ i,j=0,\ldots,n}} (t_i - t_j). \end{aligned}$$

Tím je hodnota Vandermondova determinantu dokázána pomocí matematické indukce. Všimněte si, že rovnost

$$V_{t_0,t_1,\ldots,t_n} = \prod_{\substack{i>j \\ i,j=0,\ldots,n}} (t_i - t_j)$$

platí i v případě, kdy se dva z prvků $t_0, t_1, \ldots, t_n \in \mathbf{T}$ rovnají. Vandermondova matice je tak regulární právě když jsou prvky $t_0, t_1, \ldots, t_n \in \mathbf{T}$ navzájem různé. □

Příklad 6.3 Shamirovo schéma pro sdílení tajemství

Tvrzení 6.9 *Je-li* $\mathbf{A}$ *regulární matice, pak*

$$\mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}} \cdot \operatorname{adj} \mathbf{A}.$$

Důkaz. Adjungovaná matice $\operatorname{adj} A = (n_{ij})$, kde $n_{ij} = m_{ji}$, minor matice $\mathbf{A}$ určený místem (j,i). V součinu $\mathbf{A} \cdot \operatorname{adj} \mathbf{A}$ se prvek na místě (i,i) na hlavní diagonále rovná součtu

$$\sum_{k=1}^{n} a_{ik} n_{ki} = \sum_{k=1}^{n} a_{ik} m_{ik} = \det \mathbf{A}$$

podle Věty **??**. Prvek na místě (i, j) mimo hlavní diagonálu v součinu $\mathbf{A} \cdot \operatorname{adj} \mathbf{A}$, tj. pro $i \neq j$, se rovná

$$\sum_{k=1}^{n} a_{ik} n_{kj} = \sum_{k=1}^{n} a_{ik} m_{jk}.$$

Poslední součet se rovná rozvoji determinantu podle i-tého řádku v matici, kterou dostaneme z matice $\mathbf{A}$ nahrazením j-tého řádku $\mathbf{A}_{j*}$ řádkem $\mathbf{A}_{i*}$. Minory m_{jk} pro $k = 1, \ldots, n$ se tak nezmění a nová matice má dva stejné řádky. Její determinant se proto rovná 0 podle Tvrzení **??**. Proto platí rovněž

$$\sum_{k=1}^{n} a_{ik} m_{jk} = 0.$$

Součin $\mathbf{A} \cdot \operatorname{adj} \mathbf{A}$ má proto nenulové prvky pouze na hlavní diagonále, a ty se všechny rovnají $\det \mathbf{A}$. Platí tak $\mathbf{A} \cdot \operatorname{adj} \mathbf{A} = \det \mathbf{A} \cdot \mathbf{I}_n$, neboli

$$\mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}} \cdot \operatorname{adj} \mathbf{A}.$$

□

A nakonec vzoreček pro řešení soustavy lineárních rovnic s regulární maticí. Tomuto vzorečku se říká *Cramerovo pravidlo.*

Tvrzení 6.10 *Je-li* $\mathbf{A}\mathbf{x} = \mathbf{b}$ *soustava* n *lineárních rovnic o* n *neznámých s regulární maticí* $\mathbf{A}$*, pak pro* $j = 1, 2, \ldots, n$ *platí*

$$x_j = \frac{\det \mathbf{A}_j}{\det \mathbf{A}},$$

kde $\mathbf{A}_i = [\mathbf{A}_{*1}| \cdots |\mathbf{A}_{*j-1}|\mathbf{b}|\mathbf{A}_{*j+1}| \cdots |\mathbf{A}_{*n}]$ *je matice, kterou dostaneme z matice* $\mathbf{A}$ *nahrazením* i*-tého sloupce sloupcem pravých stran* $\mathbf{b}$*.*

Důkaz. Soustava má jediné řešení $\mathbf{x} = \mathbf{A}^{-1}\mathbf{b}$. Dosadíme za inverzní matici $\mathbf{A}^{-1}$ její vyjádření podle předchozí Věty **??**

$$\mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}} \cdot \operatorname{adj} \mathbf{A}.$$

Dostaneme tak rovnost

$$\mathbf{x} = \frac{1}{\det \mathbf{A}} \cdot \operatorname{adj} \mathbf{A} \cdot \mathbf{b}.$$

Pro j-tou souřadnici řešení $\mathbf{x} = (x_1, \ldots, x_n)^T$ pak platí

$$x_j = \frac{1}{\det \mathbf{A}} \cdot [\text{adj } \mathbf{A}]_{j*}\mathbf{b} = \frac{1}{\det \mathbf{A}} \cdot \sum_{k=1}^{n} m_{kj} b_k,$$

kde b_k je k-tá souřadnice vektoru $\mathbf{b}$ pravých stran. Součet

$$\sum_{k=1}^{n} b_k m_{kj}$$

je rozvojem podle j-tého sloupce determinantu matice $\mathbf{A}_j$, kterou dostaneme z matice $\mathbf{A}$ nahrazením sloupce $\mathbf{A}_{*j}$ vektorem pravých stran $\mathbf{b}$. □

Kapitola 7

Skalární součin

V této kapitole budeme pracovat pouze nad tělesy reálných a komplexních čísel. Symbolem $\overline{x}$ budeme označovat číslo komplexně sdružené k číslu x, tj. je-li $x = a + \mathrm{i}b$, pak $\overline{x} = a - \mathrm{i}b$.

Definice 7.1 *Je-li* $\mathbf{A} = (a_{ij})$ *matice nad komplexními čísly typu* $m \times n$*, pak matici* $\mathbf{A}^* = (b_{ij})$ *typu* $n \times m$ *nazýváme* hermitovsky sdružená *k matici* $\mathbf{A}$*, pokud* $b_{ij} = \overline{a}_{ji}$ *pro každé* i, j*.*

Definice 7.2 *Jsou-li* $\mathbf{x} = (x_1, \ldots, x_n)^T$ *a* $\mathbf{y} = (y_1, \ldots, y_n)^T$ *dva aritmetické vektory z* $\mathbf{C}^n$*, pak definujeme* standardní skalární součin *vektorů* $\mathbf{x}, \mathbf{y}$ *jako číslo*

$$< \mathbf{x}, \mathbf{y} >= \mathbf{x}^*\mathbf{y} = \sum_{i=1}^{n} \overline{x}_i y_i.$$

V případě, že $\mathbf{x}, \mathbf{y}$ *jsou prvky reálného aritmetického prostoru* $\mathbf{R}^n$*, pak standardní skalární součin vektorů* $\mathbf{x}, \mathbf{y}$ *je číslo*

$$< \mathbf{x}, \mathbf{y} >= \mathbf{x}^T\mathbf{y} = \sum_{i=1}^{n} x_i y_i.$$

Tvrzení 7.1 Základní vlastnosti skalárního součinu. *Jsou-li* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbf{C}^n$ *(nebo* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbf{R}^n$*), pak platí*

1. $< \mathbf{x}, \mathbf{y} >$ *je nezáporné reálné číslo,*
2. $< \mathbf{x}, \mathbf{x} >= 0$ *právě když* $\mathbf{x} = \mathbf{0}$*,*
3. $< \mathbf{x}, a\mathbf{y} >= a < \mathbf{x}, \mathbf{y} >$ *pro každý skalár* a*,*

4. $< \mathbf{x}, \mathbf{y}+\mathbf{z} >=< \mathbf{x}, \mathbf{y} > + < \mathbf{x}, \mathbf{z} >$,

5. $< \mathbf{x}, \mathbf{y} >= \overline{< \mathbf{y}, \mathbf{x} >}$, *(nebo* $< \mathbf{x}, \mathbf{y} >=< \mathbf{y}, \mathbf{x} >$*).*

Důkaz.

1.
$$< \mathbf{x}, \mathbf{x} >= \sum_{i=1}^{n} \overline{x_i} x_i \geq 0$$
protože $\overline{x_i} x_i \geq 0 \ \forall i = 1, \ldots, n$.

2. $< \mathbf{x}, \mathbf{x} >= 0 \Leftrightarrow \overline{x_i} x_i = 0 \ \forall i \Leftrightarrow \mathbf{x} = \mathbf{0}$

3. $< \mathbf{x}, a\mathbf{y} >= \mathbf{x}^* \cdot (a\mathbf{y}) = a \cdot (\mathbf{x}^* \mathbf{y}) = a < \mathbf{x}, \mathbf{y} >$

4. $< \mathbf{x}, \mathbf{y}+\mathbf{z} >= \mathbf{x}^*(\mathbf{y}+\mathbf{z}) = \mathbf{x}^*\mathbf{y} + \mathbf{x}^*\mathbf{z} =< \mathbf{x}, \mathbf{y} > + < \mathbf{x}, \mathbf{z} >$

5.
$$\overline{< \mathbf{y}, \mathbf{x} >} = \overline{\sum_{i=1}^{n} \overline{y_i} x_i} = \sum_{i=1}^{n} \overline{x_i} y_i =< \mathbf{x}, \mathbf{y} >$$

□

Cvičení 7.1 *Dokažte pouze s použitím Tvrzení* **??**, *že platí pro každé vektory* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbf{C}^n$ *a skalár* $a \in \mathbf{C}$ *(nebo* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbf{R}^n$ *a skalár* $a \in \mathbf{R}$*)*

1. $< \mathbf{x}+\mathbf{y}, \mathbf{z} >=< \mathbf{x}, \mathbf{z} > + < \mathbf{y}, \mathbf{z} >$,

2. $< a\mathbf{x}, \mathbf{y} >= \overline{a} < \mathbf{x}, \mathbf{y} >$ *(nebo* $< a\mathbf{x}, \mathbf{y} >= a < \mathbf{x}, \mathbf{y} >$*),*

3. $< \mathbf{0}, \mathbf{x} >=< \mathbf{x}, \mathbf{0} >= 0$.

Pomocí skalárního součinu můžeme definovat délku (jinak řečeno normu) vektorů a úhel mezi nimi.

Definice 7.3 Euklidovská norma *vektoru* $\mathbf{x} = (x_1, \ldots, x_n)^T \in \mathbf{C}^n$ *je definována jako číslo*

$$\|\mathbf{x}\| = \sqrt{< \mathbf{x}, \mathbf{x} >} = \sqrt{\mathbf{x}^* \mathbf{x}} = \sqrt{\sum_{i=1}^{n} |x_i|^2}.$$

Je-li $\mathbf{x} \in \mathbf{R}^n$*, pak*

$$\|\mathbf{x}\| = \sqrt{< \mathbf{x}, \mathbf{x} >} = \sqrt{\mathbf{x}^T \mathbf{x}} = \sqrt{\sum_{i=1}^{n} x_i^2}.$$

Cvičení 7.2 *Dokažte, že pro euklidovskou normu libovolného vektoru* $\mathbf{x} \in \mathbf{C}^n$ *(nebo* $\mathbf{x} \in \mathbf{R}^n$*) a libovolný skalár* a *platí*

1. $\|\mathbf{x}\| \geq 0$,
2. $\|\mathbf{x}\| = 0$ *právě když* $\mathbf{x} = \mathbf{0}$,
3. $\|a\mathbf{x}\| = |a| \cdot \|\mathbf{x}\|$.

V následující větě dokážeme důležitou *Cauchy-Schwartzovu-Bunjakovského nerovnost.*

Věta 7.2 *Cauchy-Schwartzova-Bunjakovského nerovnost Pro libovolné dva vektory* $\mathbf{x}, \mathbf{y} \in \mathbf{C}^n$ *(nebo* $\mathbf{R}^n$*) platí*

$$| < \mathbf{x}, \mathbf{y} > | \leq \|\mathbf{x}\| \cdot \|\mathbf{y}\|,$$

rovnost nastává právě když $\mathbf{y} = a\mathbf{x}$ *pro někjaký skalár* $a \in \mathbf{C}$.

Důkaz. Je-li $\mathbf{x} = \mathbf{0}$, pak tvrzení zjevně platí. Předpokládejme tedy, že $\mathbf{x} \neq \mathbf{0}$.
Najdeme $a \in \mathbf{R}(\mathbf{C})$ takové, že $< \mathbf{x}, a\mathbf{x} - \mathbf{y} >= 0$.
$< \mathbf{x}, a\mathbf{x} - \mathbf{y} >=< \mathbf{x}, a\mathbf{x} > + < \mathbf{x}, -\mathbf{y} >= a < \mathbf{x}, \mathbf{x} > -1 \cdot < \mathbf{x}, \mathbf{y} >= 0 \Rightarrow$
$a = \frac{<\mathbf{x},\mathbf{y}>}{\|\mathbf{x}\|^2}$
$0 \leq \|a\mathbf{x} - \mathbf{y}\|^2 =< a\mathbf{x} - \mathbf{y}, a\mathbf{x} - \mathbf{y} >= a < a\mathbf{x} - \mathbf{y}, \mathbf{x} > - < a\mathbf{x} - \mathbf{y}, \mathbf{y} >= \ldots$
Poznámka: Dále pracujeme v $\mathbf{C}$.
$\ldots = a < a\mathbf{x}, \mathbf{x} > -a < \mathbf{y}, \mathbf{x} > - < a\mathbf{x}, \mathbf{y} > + < \mathbf{y}, \mathbf{y} >=$
$= a\overline{a} < \mathbf{x}, \mathbf{x} > -a < \mathbf{y}, \mathbf{x} > -\overline{a} < \mathbf{x}, \mathbf{y} > + < \mathbf{y}, \mathbf{y} >=$
$= |a|^2 \|\mathbf{x}\|^2 - (a < \mathbf{y}, \mathbf{x} > + \overline{a < \mathbf{x}, \mathbf{y} >}) + \|\mathbf{y}\|^2 = \ldots$
Dosadíme za a:

$$\ldots = \frac{| < \mathbf{x}, \mathbf{y} > |^2}{\|\mathbf{x}\|^2} - \left(\frac{< \mathbf{x}, \mathbf{y} >< \mathbf{y}, \mathbf{x} >}{\|\mathbf{x}\|^2} + \frac{< \mathbf{y}, \mathbf{x} >< \mathbf{x}, \mathbf{y} >}{\|\mathbf{x}\|^2} \right) + \|\mathbf{y}\|^2 =$$

$$= \frac{| < \mathbf{x}, \mathbf{y} > |^2}{\|\mathbf{x}\|^2} - 2 \cdot \frac{| < \mathbf{x}, \mathbf{y} > |^2}{\|\mathbf{x}\|^2} + \|\mathbf{y}\|^2 = \frac{\|\mathbf{x}\|^2 \|\mathbf{y}\|^2}{\|\mathbf{x}\|^2} - \frac{| < \mathbf{x}, \mathbf{y} > |^2}{\|\mathbf{x}\|^2} \Rightarrow$$

$$\Rightarrow 0 \leq \|\mathbf{x}\|^2 \cdot \|\mathbf{y}\|^2 - | < \mathbf{x}, \mathbf{y} > |^2 \Rightarrow | < \mathbf{x}, \mathbf{y} > | \leq \|\mathbf{x}\| \cdot \|\mathbf{y}\|$$

□

Následující trojúhelníková nerovnost platí jak pro komplexní tak pro reálné vektory.

Tvrzení 7.3 *Pro libovolné dva vektory* $\mathbf{x}, \mathbf{y} \in \mathbf{C}^n$ *(*$\mathbf{x}, \mathbf{y} \in \mathbf{R}^n$*) platí*

$$\|\mathbf{x}+\mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|.$$

Důkaz. $\|\mathbf{x}+\mathbf{y}\|^2 =< \mathbf{x}+\mathbf{y}, \mathbf{x}+\mathbf{y} >=< \mathbf{x}, \mathbf{x} > + < \mathbf{x}, \mathbf{y} > + < \mathbf{y}, \mathbf{x} > + < \mathbf{y}, \mathbf{y} >= \|\mathbf{x}\|^2 + 2Re(| < \mathbf{x}, \mathbf{y} > |) + \|\mathbf{y}\|^2 \leq \ldots$
Poznámka: $2Re(| < \mathbf{x}, \mathbf{y} > |) \leq 2\| < \mathbf{x}, \mathbf{y} > \| \leq 2\|\mathbf{x}\|\|\mathbf{y}\|$ podle Věty **??**.
$\ldots \leq \|\mathbf{x}\|^2 + 2\|\mathbf{x}\|\|\mathbf{y}\| + \|\mathbf{y}\|^2 = (\|\mathbf{x}\| + \|\mathbf{y}\|)^2$ □

Příklad 7.1 Geometrický význam skalárního součinu dvou vektorů z $\mathbf{R}^n$.

Definice 7.4 *Dva vektory* $\mathbf{x}, \mathbf{y} \in \mathbf{C}^n$ *(nebo* $\mathbf{x}, \mathbf{y} \in \mathbf{R}^n$*) nazýváme* kolmé, *platí-li* $< \mathbf{x}, \mathbf{y} >= 0$.

Definice 7.5 *Množina vektorů* $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\} \subseteq \mathbf{C}^n$ *(nebo* $\mathbf{R}^n$*) se nazývá* ortogonální, *platí-li* $< \mathbf{u}_i, \mathbf{u}_j >= 0$ *kdykoliv* $i \neq j$. *Ortogonální množina se nazývá* ortonormální, *platí-li navíc* $\|\mathbf{u}_i\| = 1$ *pro každé* $i = 1, \ldots, k$.

Tvrzení 7.4 *Každá ortogonální množina vektorů v* $\mathbf{C}^n$ *(nebo v* $\mathbf{R}^n$*) je lineárně nezávislá.*

Důkaz. Nechť $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ je ortogonální. Nechť $a_1\mathbf{x}_1 + \cdots + a_k\mathbf{x}_k = 0$. Chceme $a_1 = \cdots = a_k = 0$.

$$< \mathbf{x}_i, a_1\mathbf{x}_1 + \cdots + a_k\mathbf{x}_k >= 0 \Rightarrow \sum_{j=1}^{k} a_j < \mathbf{x}_i, \mathbf{x}_j >= 0$$

Pro $i \neq j$ jsou všechny členy rovny 0. Pokud $i = j$: $a_i < \mathbf{x}_i, \mathbf{x}_i >= 0 \Rightarrow a_i = 0 \forall i$. □

Definice 7.6 Ortonormální báze *v podprostoru* $\mathbf{P} \subseteq \mathbf{C}^n$ *(nebo* $\mathbf{P} \subseteq \mathbf{R}^n$*) je báze* $\mathbf{P}$*, která je současně ortonormální množinou.*

Tvrzení 7.5 *Buď* $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ *ortonormální báze podprostoru* $\mathbf{P}$ *prostoru* $\mathbf{C}^n$ *(nebo* $\mathbf{R}^n$*) a* $\mathbf{x} \in \mathbf{P}$. *Pak platí*

$$\mathbf{x} = \sum_{i=1}^{k} < \mathbf{u}_i, \mathbf{x} > \mathbf{u}_i.$$

Důkaz. Nechť $\mathbf{x} = a_1\mathbf{u}_1 + \cdots + a_k\mathbf{u}_k$

$$\forall i :< \mathbf{u}_i, \mathbf{x} >=< \mathbf{u}_i, \sum_{j=1}^{k} a_i\mathbf{u}_j >= \sum_{j=1}^{k} a_i < \mathbf{u}_i, \mathbf{u}_j >= a_i < \mathbf{u}_i, \mathbf{u}_i >= a_i$$

Poznámka: $< \mathbf{u}_i, \mathbf{u}_j >= 0\ \forall i \neq j, < \mathbf{u}_i, \mathbf{u}_j >= 1$ pro $i = j$. □

Definice 7.7 *Je-li* $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ *ortonormální báze podprostoru* $\mathbf{P}$ *prostoru* $\mathbf{C}^n$ *(nebo* $\mathbf{R}^n$*) a* $\mathbf{x} \in \mathbf{P}$*, pak vyjádření*

$$\mathbf{x} = \sum_{i=1}^{k} < \mathbf{u}_i, \mathbf{x} > \mathbf{u}_i.$$

nazýváme Fourierův rozklad *vektoru* $\mathbf{x}$ *vzhledem k bázi* $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ *a koeficienty* $< \mathbf{u}_i, \mathbf{x} >$ *tohoto rozkladu nazýváme* Fourierovy koeficienty *vektoru* $\mathbf{x}$ *vzhledem k bázi* $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$.

Tvrzení 7.6 *Je-li* $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ *ortonormální báze podprostoru* $\mathbf{P}$ *prostoru* $\mathbf{C}^n$ *(nebo* $\mathbf{R}^n$*) a* $\mathbf{x} = \sum_{i=1}^{k} a_i\mathbf{u}_i$, $\mathbf{y} = \sum_{i=1}^{k} b_i\mathbf{u}_i$, *pak platí*

$$< \mathbf{x}, \mathbf{y} >= \sum_{i=1}^{k} \overline{a}_i b_i.$$

Důkaz.

$$< \mathbf{x}, \mathbf{y} >=< \sum_{i=1}^{k} a_i\mathbf{u}_i, \sum_{j=1}^{k} b_j\mathbf{u}_j >= \sum_{i=1}^{k}\sum_{j=1}^{k} \overline{a_i}b_j < \mathbf{u}_i, \mathbf{u}_j >= \sum_{i=1}^{k} \overline{a_i}b_i$$

Poznámka: $< \mathbf{u}_i, \mathbf{u}_j >= 0\ \forall i \neq j, < \mathbf{u}_i, \mathbf{u}_j >= 1$ pro $i = j$. □

Kapitolu o skalárním součinu zakončíme obecnou formulací *Pythagorovy věty.*

Tvrzení 7.7 Pythagorova věta *Vektory* $\mathbf{x}, \mathbf{y} \in \mathbf{R}^n$ *jsou ortogonální právě tehdy když platí*

$$\|\mathbf{x} + \mathbf{y}\|^2 = \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2.$$

Důkaz. → Jsou-li $\mathbf{x}, \mathbf{y}$ kolmé, platí $< \mathbf{x}, \mathbf{y} >= 0$.
Potom $\|\mathbf{x} + \mathbf{y}\|^2 =< \mathbf{x} + \mathbf{y}, \mathbf{x} + \mathbf{y} >=< \mathbf{x}, \mathbf{x} > +2 < \mathbf{x}, \mathbf{y} > + < \mathbf{y}, \mathbf{y} >= \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2$.
← Pokud platí $\|\mathbf{x} + \mathbf{y}\|^2 = \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 \Rightarrow 2 < \mathbf{x}, \mathbf{y} >= 0 \Rightarrow \mathbf{x}, \mathbf{y}$ jsou na sebe kolmé.

□

Kapitola 8

Gram-Schmidtova ortogonalizace

V této kapitole budeme řešit následující úlohu.

Je dána posloupnost $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_l$ prvků lineárně nezávislé množiny $\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_l\}$ vektorů z prostoru $\mathbf{C}^n$ (nebo z $\mathbf{R}^n$). Naším úkolem je najít posloupnost $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_l$ vektorů z $\mathbf{C}^n$ (nebo z $\mathbf{R}^n$) takovou, že množina $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_l\}$ je ortonormální a navíc pro každé $k = 1, \ldots, l$ platí $\mathbf{L}\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k\} = \mathbf{L}\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\}$.

Při konstrukci ortonormální množiny $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_l\}$ budeme postupovat indukcí podle k.

Pro $k = 1$ zvolíme

$$\mathbf{u}_1 = \frac{\mathbf{x}_1}{\|\mathbf{x}_1\|}.$$

Jmenovatel zlomku je nenulový, neboť $\mathbf{x}_1 \neq \mathbf{0}$, protože lineárně nezávislá množina nemůže obsahovat nulový vektor. Dále $\|\mathbf{u}_1\| = 1$ podle Cvičení **??**.2.

Předpokládejme nyní, že pro nějaké $k \geq 1$ a $k < l$ už máme sestrojenou ortonormální množinu $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$, pro kterou platí $\mathbf{L}\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_i\} = \mathbf{L}\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_i\}$ pro každé $i = 1, \ldots, k$. Budeme hledat nutné podmínky, které musí vektor $\mathbf{u}_{k+1}$ splňovat. Vektor $\mathbf{u}_{k+1}$ musíme zvolit tak, aby platila rovnost $\mathbf{L}\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{k+1}\} = \mathbf{L}\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{k+1}\}$. Protože $\mathbf{x}_{k+1} \in \mathbf{L}\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{k+1}\} = \mathbf{L}\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{k+1}\}$ a $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{k+1}\}$ má být ortonormální báze podprostoru $\mathbf{L}\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{k+1}\}$, musí mít vektor $\mathbf{x}_{k+1}$ Fourierův rozklad podle Tvrzení **??**, tj.

$$\mathbf{x}_{k+1} = \sum_{j=1}^{k+1} < \mathbf{u}_j, \mathbf{x}_{k+1} > \mathbf{u}_j.$$

Musí být $< \mathbf{u}_{k+1}, \mathbf{x}_{k+1} > \neq 0$, v opačném případě by totiž platilo

$$\mathbf{x}_{k+1} \in \mathbf{L}\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\} = \mathbf{L}\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k\},$$

což by bylo ve sporu s lineární nezávislostí množiny vektorů $\{\mathbf{x}_1, \ldots, \mathbf{x}_{k+1}\}$. Je tedy $< \mathbf{u}_{k+1}, \mathbf{x}_{k+1} > \neq 0$ a z rovnosti pro $\mathbf{x}_{k+1}$ můžeme tedy vypočítat

$$\mathbf{u}_{k+1} = \frac{\mathbf{x}_{k+1} - \sum_{j=1}^{k} < \mathbf{u}_j, \mathbf{x}_{k+1} > \mathbf{u}_j}{< \mathbf{u}_{k+1}, \mathbf{x}_{k+1} >}.$$

Dále má být $\|\mathbf{u}_{k+1}\| = 1$, tj. musí být

$$| < \mathbf{u}_{k+1}, \mathbf{x}_{k+1} > | = \|\mathbf{x}_{k+1} - \sum_{j=1}^{k} < \mathbf{u}_j, \mathbf{x}_{k+1} > \mathbf{u}_j\|.$$

Všimněme si, že uvedenou normu známe, neboť závisí pouze na vektorech $\mathbf{u}_1, \ldots, \mathbf{u}_k$, které všechny známe na základě indukčního předpokladu. Označíme tuto normu ν_{k+1}. Dostali jsme tedy nutnou podmínku pro vyjádření vektoru $\mathbf{u}_{k+1}$:

$$\mathbf{u}_{k+1} = \frac{\mathbf{x}_{k+1} - \sum_{j=1}^{k} < \mathbf{u}_j, \mathbf{x}_{k+1} > \mathbf{u}_j}{\nu_{k+1}}.$$

Skutečnost, že tato podmínka je také postačující, je obsahem následující věty.

Věta 8.1 *Buď $\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_l\}$ lineárně nezávislá množina vektorů z $\mathbf{C}^n$ (nebo z $\mathbf{R}^n$). Položme*

$$\mathbf{u}_1 = \frac{\mathbf{x}_1}{\|\mathbf{x}_1\|}$$

a pro každé $k = 1, \ldots, l-1$

$$\mathbf{u}_{k+1} = \frac{\mathbf{x}_{k+1} - \sum_{j=1}^{k} < \mathbf{u}_j, \mathbf{x}_{k+1} > \mathbf{u}_j}{\nu_{k+1}},$$

kde $\nu_{k+1} = \|\mathbf{x}_{k+1} - \sum_{j=1}^{k} < \mathbf{u}_j, \mathbf{x}_{k+1} > \mathbf{u}_j\|$.

Potom je $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_l\}$ ortonormální množina a platí

$$\mathbf{L}\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k\} = \mathbf{L}\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\}$$

pro každé $k = 1, \ldots, l$.

Důkaz. Zřejmě $\|\mathbf{u}_i\| = 1$ pro každé $i = 1, \ldots, l$. Indukcí podle k dokážeme, že pro každé $i < k$ platí $< \mathbf{u}_i, \mathbf{u}_k >= 0$. Pro $k = 1$ toto tvrzení platí, neboť žádný vektor $\mathbf{u}_i$ pro $i < 1$ neexistuje. Předpokládejme tedy, že pro nějaké $k \geq 1$ a $k < l$ platí $< \mathbf{u}_i, \mathbf{u}_k >= 0$ pro každé $i < k$. Zvolme libovolné $i < k + 1$. Pak platí

$$\begin{aligned} < \mathbf{u}_i, \mathbf{u}_{k+1} > &= < \mathbf{u}_i, \nu_{k+1}^{-1}(\mathbf{x}_{k+1} - \sum_{j=1}^{k} < \mathbf{u}_j, \mathbf{x}_{k+1} > \mathbf{u}_j) > \\ &= \nu_{k+1}^{-1}(< \mathbf{u}_i, \mathbf{x}_{k+1} > - \sum_{j=1}^{k} < \mathbf{u}_j, \mathbf{x}_{k+1} > \cdot < \mathbf{u}_i, \mathbf{u}_j >) \\ &= \nu_{k+1}^{-1}(< \mathbf{u}_i, \mathbf{x}_{k+1} > - < \mathbf{u}_i, \mathbf{x}_{k+1} >) = 0. \end{aligned}$$

Tím je dokázáno, že $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_l\}$ je ortonormální množina. Zbývá dokázat, že

$$\mathbf{L}\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k\} = \mathbf{L}\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\}$$

pro každé $k = 1, \ldots, l$. Opět budeme postupovat indukcí podle k. Pro $k = 1$ tato rovnost zřejmě platí, neboť $\mathbf{u}_1$ je nenulovým skalárním násobkem $\mathbf{x}_1$. Předpokládejme, že pro nějaké $k \geq 1$ a $k < l$ platí $\mathbf{L}\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k\} = \mathbf{L}\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\}$. Protože

$$\mathbf{u}_{k+1} = \frac{\mathbf{x}_{k+1} - \sum_{j=1}^{k} < \mathbf{u}_j, \mathbf{x}_{k+1} > \mathbf{u}_j}{\nu_{k+1}},$$

platí $\mathbf{u}_{k+1} \in \mathbf{L}\{\mathbf{u}_1, \ldots, \mathbf{u}_k, \mathbf{x}_{k+1}\} \subseteq = -\mathbf{L}\{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{x}_{k+1}\}$ a tedy

$$\mathbf{L}\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{k+1}\} \subseteq \mathbf{L}\{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{x}_{k+1}\}.$$

Opačnou inkluzi dokážeme podobně pomocí indučního předpokladu a vyjádření

$$\mathbf{x}_{k+1} = \nu_{k+1}\mathbf{u}_{k+1} + \sum_{j=1}^{k} < \mathbf{u}_j, \mathbf{x}_{k+1} > \mathbf{u}_j.$$

□

Konstrukce množiny $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_l\}$ vede k následujícímu *klasickému Gram-Schmidtovu algoritmu.*

Algoritmus 8.1

input $\mathbf{x}_1, \ldots, \mathbf{x}_l$,
output $\mathbf{u}_1, \ldots, \mathbf{u}_l$,

$\mathbf{u}_1 \leftarrow \frac{\mathbf{x}_1}{\|\mathbf{x}_1\|}$,

for $k = 2, \ldots, l$,

$\mathbf{u}_k \leftarrow \mathbf{x}_k - \sum_{j=1}^{k-1} < \mathbf{u}_j, \mathbf{x}_k > \mathbf{u}_j$,

$\mathbf{u}_k \leftarrow \frac{\mathbf{u}_k}{\|\mathbf{u}_k\|}$.

Následující *věta o QR-rozkladu* je maticovou formulací Gram-Schmidtova algoritmu.

Věta 8.2 *Buď $\mathbf{A} = (a_{ij})$ matice typu $m \times n$ nad $\mathbf{C}$ (nebo nad $\mathbf{R}$) s lineárně nezávislými sloupci. Pak existuje matice $\mathbf{Q}$ typu $m \times n$ s ortonormálními sloupci a horní trojúhelníková matice $\mathbf{R}$ řádu n s kladnými prvky na hlavní diagonále takové, že platí $\mathbf{A} = \mathbf{QR}$.*

Důkaz. Označme $\mathbf{a}_j = \mathbf{A}_{*j}$ sloupcové vektory matice $\mathbf{A}$. Potom $\mathbf{a}_1, \ldots, \mathbf{a}_n$ je lineárně nezávislá množina vektorů z $\mathbf{C}^m$ (nebo z $\mathbf{R}^m$). Podle Věty **??** tvoří vektory $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_n$ definované jako

$$\mathbf{q}_1 = \frac{\mathbf{a}_1}{\nu_1}, \quad \nu_1 = \|\mathbf{a}_1\|$$

a

$$\mathbf{q}_k = \frac{\mathbf{a}_k - \sum_{i=1}^{k-1} < \mathbf{q}_i, \mathbf{a}_k > \mathbf{q}_i}{\nu_k}, \quad \nu_k = \|\mathbf{a}_k - \sum_{i=1}^{k-1} < \mathbf{q}_i, \mathbf{a}_k > \mathbf{q}_i\|,$$

pro $k = 2, \ldots, n$, ortonormální množinu v $\mathbf{C}^m$ ($\mathbf{R}^m$).

Vzorce definující $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_n$ přepíšeme ve tvaru

$$\begin{aligned} \mathbf{a}_1 &= \nu_1 \mathbf{q}_1, \\ \mathbf{a}_k &= \nu_k \mathbf{q}_k + < \mathbf{q}_1, \mathbf{a}_k > \mathbf{q}_1 + \cdots + < \mathbf{q}_{k-1}, \mathbf{a}_k > \mathbf{q}_{k-1} \end{aligned}$$

pro $k = 2, \ldots, n$.

Označíme-li $\mathbf{Q} = (\mathbf{q}_1 | \mathbf{q}_2 | \cdots | \mathbf{q}_n)$ a

$$\mathbf{R} = \begin{pmatrix} \nu_1 & < \mathbf{q}_1, \mathbf{a}_2 > & < \mathbf{q}_1, \mathbf{a}_3 > & \cdots & < \mathbf{q}_1, \mathbf{a}_n > \\ 0 & \nu_2 & < \mathbf{q}_2, \mathbf{a}_3 > & \cdots & < \mathbf{q}_2, \mathbf{a}_n > \\ 0 & 0 & \nu_3 & \cdots & < \mathbf{q}_3, \mathbf{a}_n > \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & < \mathbf{q}_{k-1}, \mathbf{a}_n > \\ 0 & 0 & 0 & \cdots & \nu_n \end{pmatrix},$$

pak poslední vztahy vyjadřující $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$ znamenají, že $\mathbf{A} = \mathbf{QR}$. □

Klasický Gram-Schmidtův algoritmus není numericky stabilní. Jeho stabilitu lze vylepšit (i když ne úplně zaručit) pomocí jiného uspořádání jednotlivých algebraických operací při výpočtu ortonormální množiny $\{\mathbf{u}_1, \ldots, \mathbf{u}_l\}$. Numericky stabilní procesy ortogonalizace si ukážeme v příští kapitole.

Formule

$$\mathbf{u}_1 = \frac{\mathbf{x}_1}{\|\mathbf{x}_1\|}$$

$$\mathbf{u}_k = \frac{\mathbf{x}_k - \sum_{j=1}^{k-1} < \mathbf{u}_j, \mathbf{x}_k > \mathbf{u}_j}{\|\mathbf{x}_{k+1} - \sum_{j=1}^{k-1} < \mathbf{u}_j, \mathbf{x}_k > \mathbf{u}_j\|},$$

pro každé $k = 2, \ldots, l$, si přepíšeme následovně.

Označíme $\mathbf{U}_1 = \mathbf{0}_{n\times 1}$ nulový vektor dimenze n a $\mathbf{U}_k = (\mathbf{u}_1|\mathbf{u}_2|\cdots|\mathbf{u}_{k-1})$ matici typu $n \times (k-1)$ pro $k = 2, \ldots, l$. Potom platí pro každé $k > 1$

$$\mathbf{U}_k^* \mathbf{x}_k = \begin{pmatrix} \mathbf{u}_1^* \mathbf{x}_k \\ \mathbf{u}_2^* \mathbf{x}_k \\ \vdots \\ \mathbf{u}_{k-1}^* \mathbf{x}_k \end{pmatrix} = \begin{pmatrix} < \mathbf{u}_1, \mathbf{x}_k > \\ < \mathbf{u}_2, \mathbf{x}_k > \\ \vdots \\ < \mathbf{u}_{k-1}, \mathbf{x}_k > \end{pmatrix}$$

a tedy

$$\mathbf{U}_k \mathbf{U}_k^* \mathbf{x}_k = \sum_{j=1}^{k-1} < \mathbf{u}_j, \mathbf{x}_k > \mathbf{u}_j,$$

a

$$\mathbf{x}_k - \sum_{j=1}^{k-1} < \mathbf{u}_j, \mathbf{x}_k > \mathbf{u}_j = \mathbf{x}_k - \mathbf{U}_k \mathbf{U}_k^* \mathbf{x}_k = (\mathbf{I}_n - \mathbf{U}_k \mathbf{U}_k^*)\mathbf{x}_k.$$

Při započtení toho, že $\mathbf{U}_1 = \mathbf{0}_{n\times 1}$, platí poslední rovnost pro každé $k \geq 1$. To znamená, že

$$\mathbf{u}_k = \frac{(\mathbf{I}_n - \mathbf{U}_k \mathbf{U}_k^*)\mathbf{x}_k}{\|(\mathbf{I}_n - \mathbf{U}_k \mathbf{U}_k^*)\mathbf{x}_k\|}$$

pro každé $k = 1, \ldots, l$.

Matici $\mathbf{I}_n - \mathbf{U}_k \mathbf{U}_k^*$ vyjádříme jako součin jednodušších matic. Označíme $\mathbf{E}_1 = \mathbf{I}_n$ a $\mathbf{E}_i = \mathbf{I}_n - \mathbf{u}_{i-1}\mathbf{u}_{-1}^*$ pro $i > 1$. Potom platí

$$\begin{aligned} \mathbf{E}_2\mathbf{E}_1 &= \mathbf{I}_n - \mathbf{u}_1\mathbf{u}_1^* \\ \mathbf{E}_3\mathbf{E}_2\mathbf{E}_1 &= \mathbf{I}_n - \mathbf{u}_1\mathbf{u}_1^* - \mathbf{u}_2\mathbf{u}_2^* \\ &\vdots \\ \mathbf{E}_k \cdots \mathbf{E}_3\mathbf{E}_2\mathbf{E}_1 &= \mathbf{I}_n - \mathbf{u}_1\mathbf{u}_1^* - \mathbf{u}_2\mathbf{u}_2^* - \cdots - \mathbf{u}_{k-1}\mathbf{u}_{k-1}^*, \end{aligned}$$

při výpočtu jsem použili ortogonalitu vektorů $\mathbf{u}_i$.

Vektory $\mathbf{u}_i$ získané klasickým Gram-Schmidtovým algoritmem tak můžeme vyjádřit ve tvaru

$$\mathbf{u}_i = \frac{\mathbf{E}_k \cdots \mathbf{E}_2 \mathbf{E}_1 \mathbf{x}_k}{\|\mathbf{E}_k \cdots \mathbf{E}_2 \mathbf{E}_1 \mathbf{x}_k\|}$$

pro $k = 1, 2, \ldots, l$.

Uvedené vyjádření vektorů $\mathbf{u}_i$ vede k následujícímu *modifikovanému Gram-Schmidtovu algoritmu.*

Algoritmus 8.2

input $\mathbf{x}_1, \ldots, \mathbf{x}_l$,
output $\mathbf{u}_1, \ldots, \mathbf{u}_l$,

$\mathbf{u}_1 \leftarrow \frac{\mathbf{x}_1}{\|\mathbf{x}_1\|}$,

for $k = 2, \ldots, l$,

for $j = k, \ldots, l$,

$\mathbf{u}_j \leftarrow \mathbf{E}_k \mathbf{u}_j$,

$\mathbf{u}_k \leftarrow \frac{\mathbf{u}_k}{\|\mathbf{u}_k\|}$.

Důkaz posledního tvrzení této kapitoly vyplývá z výpočtů před formulací modifikovaného Gram-Schmidtova algoritmu.

Tvrzení 8.3 *Modifikovaný Gram-Schmidtův algoritmus vede ke stejné ortonormální posloupnosti* $\mathbf{u}_1, \ldots, \mathbf{u}_l$ *jako klasický Gram-Schmidtův algoritmus.*

Ani modifikovaný Gram-Schmidtův algoritmus není numericky stabilní pro všechny typy úloh. Nicméně je o něco stabilnější než klasický algoritmus. Můžete si to ověřit v následující úloze.

Úloha 8.1

Použijte aritmetiku s plovoucí čárkou, která zaokrouhluje na tři platná místa a obě varianty Gram-Schmidtova algoritmu k ortogonalizaci posloupnosti vektorů $\mathbf{x}_1 = (1, 10^{-3}, 10^{-3})^T$, $\mathbf{x}_2 = (1, 10^{-3}, 0)^T$ a $\mathbf{x}_3 = (1, 0, 10^{-3})^T$. Zatímco modifikovaný Gram-Schmidtův algoritmus dává tři vektory, které jsou tak ortonormální, jak jen to je v aritmetice zaokrouhlující na tři platná místa možné, u klasického Gram-Schmidtova algoritmu druhý a třetí vektor nejsou příliš kolmé.

Kapitola 9

Ortogonální a unitární matice

Také v této kapitole budeme pracovat pouze nad tělesy reálných a komplexních čísel.

Definice 9.1 *Čtvercová matice* $\mathbf{U}$ *řádu* n *nad* $\mathbf{C}$ *(nebo nad* $\mathbf{R}$*) se nazývá unitární (nebo ortogonální), tvoří-li její sloupce ortonormální množinu vektorů v* $\mathbf{C}^n$ *(nebo v* $\mathbf{R}^n$*).*

Věta 9.1 *Buď* $\mathbf{U}$ *čtvercová matice řádu* n *nad* $\mathbf{C}$ *(nebo* $\mathbf{R}$*). Následující podmínky jsou ekvivalentní:*

1. *matice* $\mathbf{U}$ *unitární (nebo ortogonální),*
2. *matice* $\mathbf{U}$ *má ortonormální řádky,*
3. $\mathbf{U}^*\mathbf{U} = \mathbf{I}_n$*, tj.* $\mathbf{U}^{-1} = \mathbf{U}^*$ *(*$\mathbf{U}^T\mathbf{U} = \mathbf{I}^n$ *v případě reálné matice),*
4. $\|\mathbf{U}\mathbf{x}\| = \|\mathbf{x}\|$ *pro každý vektor* $\mathbf{x} \in \mathbf{C}^n$ *(nebo* $\mathbf{x} \in \mathbf{R}^n$*).*

Důkaz. Dokážeme pouze pro komplexní matici $\mathbf{U}$. V případě reálné matice $\mathbf{U}$ jsou důkazy analogické, v případě implikace 4. $\Rightarrow$ 1. je důkaz dokonce mnohem snazší.

Zřejmě 1. je ekvivalentní s 3. Stejně tak 2. je ekvivalentní s rovností $\mathbf{U}\mathbf{U}^* = \mathbf{I}_n$, která je zase ekvivalentní s 3. v případě čtvercových matic. (Proč?)

1. $\Rightarrow$ 4. Platí $\|\mathbf{U}\mathbf{x}\|^2 = (\mathbf{U}\mathbf{x})^*\mathbf{U}\mathbf{x} = \mathbf{x}^*\mathbf{U}^*\mathbf{U}\mathbf{x} = \mathbf{x}^*\mathbf{x} = \|\mathbf{x}\|^2$.

4. $\Rightarrow$ 1. Pro každý vektor $\mathbf{e}_j$ standardní báze v $\mathbf{C}^n$ platí $\mathbf{U}_{*j} = \mathbf{U}\mathbf{e}_j$. Potom $\|\mathbf{U}_{*j}\|^2 = \|\mathbf{U}\mathbf{e}_j\|^2 = \|e_j\|^2 = 1$, tj. $\|\mathbf{U}_{*j}\| = 1$. Dále platí pro $j \neq k$, že $\mathbf{U}_{*j}^* \mathbf{U}_{*k} = \mathbf{e}_j^* \mathbf{U}^* \mathbf{U}\mathbf{e}_k$. Zbývá tedy dokázat, že $\mathbf{e}_j^* \mathbf{U}^* \mathbf{U}\mathbf{e}_k = 0$ pro $j \neq k$.

Použitím podmínky 4. na vektor $\mathbf{e}_j + \mathbf{e}_k$ dostaneme

$$\begin{aligned}(\mathbf{e}_j + \mathbf{e}_k)^* \mathbf{U}^* \mathbf{U}(\mathbf{e}_j + \mathbf{e}_k) &= \|\mathbf{U}(\mathbf{e}_j + \mathbf{e}_k)\|^2 = \|\mathbf{e}_j + \mathbf{e}_k\|^2 \\ &= \|\mathbf{e}_j\|^2 + \|\mathbf{e}_k\|^2 = 2,\end{aligned}$$

neboť vektory $\mathbf{e}_j, \mathbf{e}_k$ jsou kolmé a platí Pythagorova věta. Roznásobením a dvojím použitím předpokladu 4. dále dostaneme

$$\begin{aligned}(\mathbf{e}_j + \mathbf{e}_k)^* \mathbf{U}^* \mathbf{U}(\mathbf{e}_j + \mathbf{e}_k) &= \mathbf{e}_j^* \mathbf{U}^* \mathbf{U}\mathbf{e}_k + \mathbf{e}_k^* \mathbf{U}^* \mathbf{U}\mathbf{e}_j + \mathbf{e}_j^* \mathbf{U}^* \mathbf{U}\mathbf{e}_j + \mathbf{e}_k^* \mathbf{U}^* \mathbf{U}\mathbf{e}_k \\ &= \mathbf{e}_j^* \mathbf{U}^* \mathbf{U}\mathbf{e}_k + (\mathbf{e}_j^* \mathbf{U}^* \mathbf{U}\mathbf{e}_k)^* + \|\mathbf{U}\mathbf{e}_j\|^* + \|\mathbf{U}\mathbf{e}_k\|^2 \\ &= 2\,\mathrm{Re}\,(\mathbf{e}_j^* \mathbf{U}^* \mathbf{U}\mathbf{e}_k) + \|\mathbf{e}_j\|^2 + \|\mathbf{e}_k\|^2 \\ &= 2\,\mathrm{Re}\,(\mathbf{e}_j^* \mathbf{U}^* \mathbf{U}\mathbf{e}_k) + 2.\end{aligned}$$

Srovnáním výsledků obou posledních výpočtů dostáváme

$$\mathrm{Re}\,(\mathbf{e}_j^* \mathbf{U}^* \mathbf{U}\mathbf{e}_k) = 0$$

Tytéž výpočty provedeme s vektorem $\mathbf{e}_j + \mathrm{i}\mathbf{e}_k$.

$$\begin{aligned}(\mathbf{e}_j + \mathrm{i}\mathbf{e}_k)^* \mathbf{U}^* \mathbf{U}(\mathbf{e}_j + \mathrm{i}\mathbf{e}_k) &= \|\mathbf{U}(\mathbf{e}_j + \mathrm{i}\mathbf{e}_k)\|^2 = \|\mathbf{e}_j + \mathrm{i}\mathbf{e}_k\|^2 \\ &= \|\mathbf{e}_j\|^2 + \|\mathrm{i}\mathbf{e}_k\|^2 = 2,\end{aligned}$$

a

$$\begin{aligned}&(\mathbf{e}_j + \mathrm{i}\mathbf{e}_k)^* \mathbf{U}^* \mathbf{U}(\mathbf{e}_j + \mathrm{i}\mathbf{e}_k) \\ = \;& \mathbf{e}_j^* \mathbf{U}^* \mathbf{U}(\mathrm{i}\mathbf{e}_k) + (\mathrm{i}\mathbf{e}_k)^* \mathbf{U}^* \mathbf{U}\mathbf{e}_j + \mathbf{e}_j^* \mathbf{U}^* \mathbf{U}\mathbf{e}_j + (\mathrm{i}\mathbf{e}_k)^* \mathbf{U}^* \mathbf{U}(\mathrm{i}\mathbf{e}_k) \\ = \;& \mathrm{i}(\mathbf{e}_j^* \mathbf{U}^* \mathbf{U}\mathbf{e}_k) - \mathrm{i}(\mathbf{e}_k^* \mathbf{U}^* \mathbf{U}\mathbf{e}_j) + \|\mathbf{U}\mathbf{e}_j\|^* + \|\mathbf{U}(\mathrm{i}\mathbf{e}_k)\|^2 \\ = \;& 2\,\mathrm{i}\,\mathrm{Im}\,(\mathbf{e}_j^* \mathbf{U}^* \mathbf{U}\mathbf{e}_k) + \|\mathbf{e}_j\|^2 + \|\mathbf{e}_k\|^2 \\ = \;& 2\,\mathrm{i}\,\mathrm{Im}\,(\mathbf{e}_j^* \mathbf{U}^* \mathbf{U}\mathbf{e}_k) + 2,\end{aligned}$$

tj.

$$\mathrm{Im}\,(\mathbf{e}_j^* \mathbf{U}^* \mathbf{U}\mathbf{e}_k) = 0.$$

Proto $\mathbf{e}_j^* \mathbf{U}^* \mathbf{U}\mathbf{e}_k = \mathbf{U}_{*j}^* \mathbf{U}_{*k} = 0$ pro libovolné $j \neq k$. □

Tvrzení 9.2 *Součin unitárních (ortogonálních) matic je unitární (ortogonální) matice.*

Důkaz. Nechť $\mathbf{U}, \mathbf{V}$ jsou unitární matice řádu n.
Potom platí $\mathbf{U}^*\mathbf{U} = \mathbf{I}_n = \mathbf{V}^*\mathbf{V}$.
Protože platí $(\mathbf{UV})^*\mathbf{UV} = \mathbf{V}^*\mathbf{U}^*\mathbf{UV} = \mathbf{V}^*\mathbf{V} = \mathbf{I}_n$, je podle Věty **??**.2 $\mathbf{UV}$ unitární.
Analogicky pro ortogonální matice nad $\mathbf{R}$. □

Věta 9.3 *Je-li* $\mathbf{A}$ *regulární matice a* $\mathbf{A} = \mathbf{QR}$ *její QR-rozklad, pak jsou matice* $\mathbf{Q}$ *a* $\mathbf{R}$ *určené jednoznačně.*

Důkaz. Předpokládejme, že $\mathbf{A} = \mathbf{Q}_1\mathbf{R}_1 = \mathbf{Q}_2\mathbf{R}_2$ (splňující předpoklady).
$\Rightarrow \mathbf{Q}_2^T\mathbf{Q}_1 = \mathbf{R}_2\mathbf{R}_1^{-1} = \mathbf{U} = (u_{ij})$
ortogonální matice = horní trojúhelníková matice s kladnými prvky na hlavní diagonále:

$$\mathbf{U} = \begin{pmatrix} u_{11} & u_{12} & \dots & u_{1n} \\ 0 & u_{22} & \dots & \vdots \\ \vdots & 0 & \ddots & \vdots \\ 0 & \dots & 0 & u_{nn} \end{pmatrix}$$

$\mathbf{U}$ je ortogonální, tedy $u_{11}^2 = 1$, navíc víme, že $u_{11} > 0$, tedy $u_{11} = 1$.
Označíme $\mathbf{u}_i$ i-tý sloupec matice $\mathbf{U}$, pak
$(\mathbf{u}_1^T\mathbf{u}_2 = u_{11}u_{12} = 0 \wedge u_{11} = 1) \Rightarrow u_{12} = 0$
$\mathbf{u}_2\mathbf{u}_2 = u_{22}^2 = 1$ atd.
Tedy $u_{ii} = 1\ \forall i = 1, \dots, n$ a $u_{ij} = 0\ \forall i \neq j$, tedy $\mathbf{U} = \mathbf{I}_n$.
Protože matice $\mathbf{Q}_1, \mathbf{Q}_2$ jsou ortogonální, z rovnosti $\mathbf{Q}_2^T\mathbf{Q}_1 = \mathbf{I}_n$ vyplývá, že $\mathbf{Q}_1 = \mathbf{Q}_2$, tedy i $\mathbf{R}_1 = \mathbf{R}_2$. □

Definice 9.2 *Je-li* $X \subseteq \mathbf{C}^n$ *(nebo* $\mathbf{R}^n$*) pak definujeme* ortogonální doplněk *množiny* X *jako množinu*

$$X^\perp = \{\mathbf{y} :< \mathbf{x}, \mathbf{y} >= 0 \text{ pro každý vektor } \mathbf{x} \in X\}.$$

V případě jednoprvkové množiny $X = \{\mathbf{u}\}$ budeme ortogonální doplněk $\{\mathbf{u}\}$ označovat $\mathbf{u}^\perp$.

Tvrzení 9.4 *Pro libovolné dvě podmnožiny* $X, Y \subseteq \mathbf{C}^n$ *(nebo* $\mathbf{R}^n$*) platí*

1. $X^\perp$ *je podprostor* $\mathbf{C}^n$ *(nebo* $\mathbf{R}^n$*),*
2. *z* $X \subseteq Y$ *plyne* $Y^\perp \subseteq X^\perp$,

3. $X^{\perp} = \mathbf{L}(X)^{\perp}$,

4. *je-li* $\mathbf{P}$ *podprostor* $\mathbf{C}^n$ *(nebo* $\mathbf{R}^n$*), pak* $(\mathbf{P}^{\perp})^{\perp} = \mathbf{P}$,

5. *pro podprostor* $\mathbf{P}$ *platí* $\mathbf{P} \cap \mathbf{P}^{\perp} = \{\mathbf{0}\}$,

6. *každý prvek* $\mathbf{x} \in \mathbf{C}^n$ *(nebo* $\mathbf{R}^n$*) lze jednoznačně vyjádřit ve tvaru* $\mathbf{x} = \mathbf{p} + \mathbf{q}$, *kde* $\mathbf{p} \in \mathbf{P}$ *a* $\mathbf{q} \in \mathbf{P}^{\perp}$,

7. $(X^{\perp})^{\perp} = \mathbf{L}(X)$.

Důkaz.
1. Je-li $\mathbf{u}, \mathbf{v} \in X^{\perp}$ a $\mathbf{x} \in X$, potom:
$< \mathbf{x}, \mathbf{u} + \mathbf{v} >=< \mathbf{x}, \mathbf{u} > + < \mathbf{x}, \mathbf{v} >= 0 + 0 = 0.$
Je-li $a \in \mathbf{R}(\mathbf{C})$, potom
$< \mathbf{x}, a\mathbf{u} >= a < \vec{,}\mathbf{u} >= a \cdot 0 = 0.$
Tedy $X^{\perp}$ je podprostor$\mathbf{R}^n(\mathbf{C}^n)$.
2. Je-li $X \subseteq Y$ a $\mathbf{z} \in Y^{\perp}$, potom
$(< \mathbf{y}, \mathbf{z} >= 0 \quad \forall \mathbf{y} \in Y) \Rightarrow (< \mathbf{y}, \mathbf{z} >= 0 \quad \forall \mathbf{y} \in X) \Rightarrow \mathbf{z} \in X^{\perp} \Rightarrow Y^{\perp} \subseteq X^{\perp}$
3. $\mathbf{x} \in \mathbf{L}(X) \overset{2}{\Rightarrow} \mathbf{L}(X)^{\perp} \subseteq X^{\perp}$
Je-li $\mathbf{z} \in X^{\perp} \Rightarrow < \mathbf{z}, \mathbf{x} >= 0 \quad \forall \mathbf{x} \in X$. Je-li $\mathbf{y} \in \mathbf{L}(X)$, pak

$$\mathbf{y} = \sum_{i=1}^{n} a_i \mathbf{x}_i$$

kde $\mathbf{x}_i \in X, a_i \in \mathbf{C}(\mathbf{R})$.

$$< \mathbf{z}, \mathbf{y} >=< \mathbf{x}, \sum_{i=1}^{n} a_i \mathbf{x}_i >= \sum_{i=1}^{n} a_i < \mathbf{z}, \mathbf{x}_i >= 0$$

$\Rightarrow \mathbf{z} \in \mathbf{L}(X)^{\perp} \Rightarrow \mathbf{L}(X)^{\perp} \supseteq X^{\perp}$
4. Zvolíme bázi $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ v $\mathbf{P}$, doplníme ji do báze $\{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{x}_{k+1}, \ldots, \mathbf{x}_n\}$ v $\mathbf{C}^n(\mathbf{R}^n)$. Pomocí Gram-Schmidtovy ortogonalizace najdeme ortonormální bázi $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ v $\mathbf{C}^n(\mathbf{R}^n)$.
Pro tu platí, že $\mathbf{L}(\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}) = \mathbf{L}(\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}) = \mathbf{P}$.
Dokážeme, že $\mathbf{P}^{\perp} = \mathbf{L}(\{\mathbf{u}_{k+1}, \ldots, \mathbf{u}_n\})$.
$\forall \mathbf{u}_j, j = (k+1), \ldots, n :< \mathbf{u}_j, \mathbf{u}_i >= 0$ pro $i = 1, \ldots, k$,
tedy $\mathbf{u}_j \in \{\mathbf{u}_1, \ldots, \mathbf{u}_k\}^{\perp} \overset{3}{=} \mathbf{L}(\{\mathbf{u}_1, \ldots, \mathbf{u}_k\})^{\perp} = \mathbf{P}^{\perp}$
Tím jsme dokázali, že $\mathbf{L}(\{\mathbf{u}_{k+1}, \ldots, \mathbf{u}_n\}) \subseteq \mathbf{P}^{\perp}$.
Zvolíme $\mathbf{x} \in \mathbf{P}^{\perp}$, pak platí (podle Tvrzení **??**):

$$\mathbf{x} = \sum_{i=1}^{n} < \mathbf{u}_i, \mathbf{x} > \mathbf{u}_i$$

pro $i = 1, \ldots, k < \mathbf{u}_i, \mathbf{x} >= 0$ (protože $\mathbf{x} \in \mathbf{P}^\perp$ a $\mathbf{u}_1, \ldots, \mathbf{u}_k \in \mathbf{P}$), tedy

$$\mathbf{x} = \sum_{i=k+1}^{n} < \mathbf{u}_i, \mathbf{x} > \mathbf{u}_i \in \mathbf{L}(\{\mathbf{u}_{k+1}, \ldots, \mathbf{u}_n\})$$

Tím jsme dokázali, že $\mathbf{L}(\{\mathbf{u}_{k+1}, \ldots, \mathbf{u}_n\}) \supseteq \mathbf{P}^\perp$.
Tedy $\mathbf{L}(\{\mathbf{u}_{k+1}, \ldots, \mathbf{u}_n\}) = \mathbf{P}^\perp$.
5. $\mathbf{x} \in \mathbf{P} \cap \mathbf{P}^\perp \Rightarrow < \mathbf{x}, \mathbf{x} >= 0 \Leftrightarrow \mathbf{x} = \mathbf{0}$
6. Najdeme ortonormální bázi $\{\mathbf{u}_1, dots, \mathbf{u}_n\}$ v $\mathbf{C}^n(\mathbf{R}^n)$ takovou, že $\{\mathbf{u}_1, dots, \mathbf{u}_k\}$ je báze $\mathbf{P}$. Je-li $\mathbf{x} \in \mathbf{C}^n(\mathbf{R}^n)$, pak:

$$\mathbf{x} = \sum_{i=1}^{k} < \mathbf{u}_i, \mathbf{x} > \mathbf{u}_i + \sum_{i=k+1}^{n} < \mathbf{u}_i, \mathbf{x} > \mathbf{u}_i$$

Položíme

$$\mathbf{p} = \sum_{i=1}^{k} < \mathbf{u}_i, \mathbf{x} > \mathbf{u}_i \in \mathbf{P}, \mathbf{q} = \sum_{i=k+1}^{n} < \mathbf{u}_i, \mathbf{x} > \mathbf{u}_i \in \mathbf{P}^\perp$$

Jednozačnost: Je-li $\mathbf{x} = \mathbf{p}_1 + \mathbf{q}_1 = \mathbf{p}_2 + \mathbf{q}_2$, kde $\mathbf{p}_1, \mathbf{p}_2 \in \mathbf{P}$ a $\mathbf{q}_1, \mathbf{q}_2 \in \mathbf{P}^\perp$, pak
$\mathbf{p}_1 - \mathbf{p}_2 = \mathbf{q}_1 - \mathbf{q}_2 \overset{5}{\Rightarrow} \mathbf{p}_1 - \mathbf{p}_2 = \mathbf{0} = \mathbf{q}_1 - \mathbf{q}_2$
7. Platí, že $X^\perp = \mathbf{L}(X)^\perp$ podle 3. Označíme $\mathbf{P} = \mathbf{L}(X)^\perp$ podprostor $\mathbf{C}^n(\mathbf{R}^n)$. Pak podle 4. $\mathbf{P}^\perp = (\mathbf{L}(X)^\perp)^\perp = \mathbf{L}(X)$. Protože $\mathbf{P} = \mathbf{L}(X)^\perp$, $(X^\perp)^\perp = (\mathbf{L}(X)^\perp)^\perp = \mathbf{L}(X)$. □

Definice 9.3 *Je-li* $\mathbf{u} \in \mathbf{C}^n$ *(nebo* $\mathbf{R}^n$*),* $\|\mathbf{u}\| = 1$*, pak matici* $\mathbf{I}_n - \mathbf{u}\mathbf{u}^*$ *(nebo* $\mathbf{I}_n - \mathbf{u}\mathbf{u}^T$*) nazýváme elementární projektor určený vektorem* $\mathbf{u}$*.*

Tvrzení 9.5 *Buď* $\mathbf{Q}$ *elementární projektor určený vektorem* $\mathbf{u} \in \mathbf{C}^n$ *(nebo* $\mathbf{R}^n$*). Pak platí*

1. $\mathbf{Q}^2 = \mathbf{Q}$,
2. $\mathbf{Q}\mathbf{x} \in \mathbf{u}^\perp$ *pro každý vektor* $\mathbf{x} \in \mathbf{C}^n$ *(nebo* $\mathbf{R}^n$*),*
3. $(\mathbf{I}_n - \mathbf{Q})\mathbf{x} \in \mathbf{L}(\mathbf{u})$.

Důkaz.
1. $\mathbf{Q}^2 = (\mathbf{I}_n - \mathbf{u}\mathbf{u}^*)^2 = \mathbf{I}_n\mathbf{I}_n - 2\mathbf{u}\mathbf{u}^* + \mathbf{u}\mathbf{u}^*\mathbf{u}\mathbf{u}^* = \mathbf{I}_n - 2\mathbf{u}\mathbf{u}^* + \mathbf{u}\mathbf{u}^* = \mathbf{I}_n - \mathbf{u}\mathbf{u}^*$
Poznámka: $\mathbf{u}\mathbf{u}^* = 1$, protože $\|\mathbf{u}\| = 1$.

2. $\mathbf{Qx} = (\mathbf{I}_n - \mathbf{uu}^*)\mathbf{x} = \mathbf{x} - \mathbf{uu}^*\mathbf{x} = \mathbf{x} - (\mathbf{u}^*\mathbf{x})\mathbf{u}$
Poznámka: $\mathbf{u}^*\mathbf{x} \in \mathbf{C}(\mathbf{R})$ je číslo.
$< \mathbf{Qx}, \mathbf{u} >= \mathbf{u}^*\mathbf{Qx} = \mathbf{u}^*[\mathbf{x} - (\mathbf{u}^*\mathbf{x})\mathbf{u}] = \mathbf{u}^*\mathbf{x} - \mathbf{u}^*\mathbf{x}\mathbf{u}^*\mathbf{u} = 0 \Rightarrow \mathbf{Qx} \in \mathbf{u}^\perp$
3. $(\mathbf{I}_n - \mathbf{Q})\mathbf{x} = \mathbf{x} - \mathbf{Qx}$
$\mathbf{x} = (\mathbf{x} - \mathbf{Qx}) + \mathbf{Qx}$, $\mathbf{Qx} \in \mathbf{u}^\perp$
$\mathbf{Qx} = \mathbf{x} - (\mathbf{u}^*\mathbf{x})\mathbf{u}$ (z 2.)
$\mathbf{x} - \mathbf{Qx} = \mathbf{x} - \mathbf{x} + (\mathbf{u}^*\mathbf{x})\mathbf{u} = (\mathbf{u}^*\mathbf{x})\mathbf{u} \in \mathbf{L}(\mathbf{u})$ □

Definice 9.4 *Buď* $\mathbf{u}$ *nenulový vektor z* $\mathbf{C}^n$ *(nebo* $\mathbf{R}^n$*). Matici*

$$\mathbf{R} = \mathbf{I}_n - \frac{2\mathbf{uu}^*}{\mathbf{u}^*\mathbf{u}} \text{ nebo } \mathbf{R} = \mathbf{I}_n - \frac{2\mathbf{uu}^T}{\mathbf{u}^T\mathbf{u}}$$

nazýváme elementární (Householderův) reflektor *určený vektorem* $\mathbf{u}$.

Tvrzení 9.6 *Buď* $\mathbf{R}$ *elementární reflektor určený vektorem* $\mathbf{u} \in \mathbf{C}^n$ *(nebo* $\mathbf{R}^n$*), pak platí*

1. $\mathbf{R}^2 = \mathbf{I}_n$, *tj.* $\mathbf{R}^{-1} = \mathbf{R}$,
2. $\mathbf{R}^* = \mathbf{R}$ *(nebo* $\mathbf{R}^T = \mathbf{R}$*), tj.* $\mathbf{R}$ *je unitární (nebo ortogonální) matice.*

Důkaz.
1. $\mathbf{R}^2 = \left(\mathbf{I}_n - 2\frac{\mathbf{uu}^*}{\mathbf{u}^*\mathbf{u}}\right)^2 = \mathbf{I}_n - 4\frac{\mathbf{uu}^*}{\mathbf{u}^*\mathbf{u}} + 4\frac{\mathbf{uu}^*\mathbf{uu}^*}{\|\mathbf{u}\|^4} = \mathbf{I}_n - 4\frac{\mathbf{uu}^*}{\mathbf{u}^*\mathbf{u}} + 4\frac{\mathbf{uu}^*}{\mathbf{u}^*\mathbf{u}} = \mathbf{I}_n$
2. $\mathbf{R}^* = \left(\mathbf{I}_n - 2\frac{\mathbf{uu}^*}{\|\mathbf{u}\|^2}\right)^* = \mathbf{I}_n - \frac{2(\mathbf{uu}^*)^*}{\|\mathbf{u}\|^2} = \mathbf{I}_n - \frac{2(\mathbf{u}^*)^*\mathbf{u}^*}{\|\mathbf{u}\|^2} = \mathbf{I}_n - 2\frac{\mathbf{uu}^*}{\|\mathbf{u}\|^2} = \mathbf{R}$
Podle Věty **??** je $\mathbf{R}$ unitární(ortogonální). □

Příklad 9.1 Matice rotací kolem souřadných os v $\mathbf{R}^3$.

Definice 9.5 Rovinná (Givensova) rotační matice *je matice řádu n*

$$\mathbf{P}_{ij} = (a_{kl}) = \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & c & \cdots & s & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & -s & \cdots & c & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix},$$

kde c, s *jsou komplexní (nebo reálná) čísla taková, že* $c^2 + s^2 = 1$. *Konkrétněji,* $a_{ii} = a_{jj} = c$, $a_{ji} = -s$, $a_{ij} = s$, *všechny ostatní prvky na hlavní diagonále se rovnají* 1 *a všechny ostatní prvky mimo hlavní diagonálu se rovnají* 0.

Jednoduchým výpočtem zjistíme, že je-li $\mathbf{x} = (x_1, \ldots, x_n)^T$, pak

$$\mathbf{P}_{ij}\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ cx_i + sx_j \\ \vdots \\ -sx_i + cx_j \\ \vdots \\ x_n \end{pmatrix}.$$

Přímým výpočtem se dokáže

Lemma 9.7 *Rovinná Givensova rotační matice je unitární (ortogonální) matice.*

Důkaz. Musíme dokázat, že sloupce $\mathbf{P}_{ij}$ tvoří ortonormální bázi v $\mathbf{R}^n$
1. velikost: Označme $\mathbf{p}_k$ k-tý sloupec matice $\mathbf{P}_{ij}$, pak $\|\mathbf{p}_k\| = 1$ pro $k \neq i, j$ (platí triviálně, potože jsou to prvky standardní báze) a $\|\mathbf{p}_k\| = c^2 + s^2 = 1$ pro $k = i, j$.
2. kolmost: Platí, že $< \mathbf{p}_k, \mathbf{p}_l >= 0$ pro $k, l \neq i, j \wedge k \neq l$, protože jsou to prvky standardní báze. Také zjevně platí $< \mathbf{p}_k, \mathbf{p}_i >=< \mathbf{p}_k, \mathbf{p}_j >= 0$ pro $k \neq i, j$. Nakonec $< \mathbf{p}_i, \mathbf{p}_j >= cs - cs = 0$. □

Tvrzení 9.8 *Pro každý nenulový vektor* $\mathbf{x} = (x_1, \ldots, x_n)^T \in \mathbf{C}^n$ *(nebo* $\mathbf{R}^n$*) platí*

$$\mathbf{P}_{in} \cdots \mathbf{P}_{i2}\mathbf{P}_{i1} = \|\mathbf{x}\|\, \mathbf{e}_i.$$

Důkaz. BÚNO předpokládejme, že $i = 1$. Potom je-li $x_1^2 + x_2^2 \neq 0$, zvolíme $c = \frac{x_1}{\sqrt{x_1^2+x_2^2}}$, $s = \frac{x_2}{\sqrt{x_1^2+x_2^2}}$.

$$\mathbf{P}_{12}\mathbf{x} = \begin{pmatrix} \sqrt{x_1^2 + x_2^2} \\ 0 \\ x_3 \\ \vdots \\ x_n \end{pmatrix}$$

Zvolíme $c = \frac{\sqrt{x_1^2+x_2^2}}{\sqrt{x_1^2+x_2^2+x_3^2}}$, $s = \frac{x_3}{\sqrt{x_1^2+x_2^2+x_3^2}}$

$$\mathbf{P}_{13}\mathbf{P}_{12}\mathbf{x} = \begin{pmatrix} \sqrt{x_1^2+x_2^2+x_3^2} \\ 0 \\ 0 \\ x_4 \\ \vdots \\ x_n \end{pmatrix}$$

Postupě tak volíme matice $\mathbf{P}_{1k}$ pro $k = 1, \ldots, n$, kde $c_k = \frac{\sqrt{x_1^2+\cdots+x_{k-1}^2}}{\sqrt{x_1^2+\cdots+x_k^2}}$, $s_k = \frac{x_k}{\sqrt{x_1^2+\cdots+x_k^2}}$. Je-li $x_1^2+x_2^2 = 0$, pak zvolíme c a s libovolně tak, aby $c^2+s^2 = 1$ a pokračujeme dokud nenrazíme na první nenulový prvek (například j-tý). Pak máme matici $\mathbf{P}_{1j}$, čísla c, s volíme analogicky jako v první části důkazu. □

Tvrzení 9.9 *Buď* $\mathbf{x} \in \mathbf{C}^n$, $\mathbf{u} = \mathbf{x} \pm \mu \|\mathbf{x}\| \mathbf{e}_1$, *kde*

$$\mu = \begin{cases} 1, & \text{pokud} \quad x_1 \in \mathbf{R}, \\ \frac{x_1}{|x_1|}, & \text{pokud} \quad x_1 \in \mathbf{C}-\mathbf{R}. \end{cases}$$

Je-li $\mathbf{R}$ *Householderův reflektor určený vektorem* $\mathbf{u}$, *tj.* $\mathbf{R} = \mathbf{I}_n - 2\frac{\mathbf{u}\mathbf{u}^*}{\mathbf{u}^*\mathbf{u}}$, *potom platí* $\mathbf{R}\mathbf{x} = \mp\mu\|\mathbf{x}\|\mathbf{e}_1$

Důkaz.

$$\mathbf{R}\mathbf{x} = \left(\mathbf{I}_n - 2\frac{\mathbf{u}\mathbf{u}^*}{\mathbf{u}^*\mathbf{u}}\right)\mathbf{x} = \mathbf{x} - 2\frac{\mathbf{u}\mathbf{u}^*\mathbf{x}}{\mathbf{u}^*\mathbf{u}} = \mathbf{x}\frac{2\mathbf{u}^*\mathbf{x}}{\mathbf{u}^*\mathbf{u}} \cdot \mathbf{u}$$

Poznámka: $\mathbf{u}^*\mathbf{x}$, $\mathbf{u}^*\mathbf{u}$ jsou čísla, $\frac{2\mathbf{u}^*\mathbf{x}}{\mathbf{u}^*\mathbf{u}}$ je koeficient u $\mathbf{u}$. Dokážeme, že $\frac{2\mathbf{u}^*\mathbf{x}}{\mathbf{u}^*\mathbf{u}} = 1$

$$\mathbf{u}^*\mathbf{x} = (x_1 \pm \mu\|\mathbf{x}\|)^* \cdot x_1 + \sum_{i=2}^{n} \overline{x_i}x_i = \overline{x_1}x_1 + \sum_{i=2}^{n} \overline{x_i}x_i \pm \mu\|\mathbf{x}\|x_1 = \|\mathbf{x}\|^2 \pm \frac{\overline{x_1}x_1}{|x_1|} \cdot \|\mathbf{x}\| =$$

$$= \begin{cases} x_1 \in \mathbf{C} & \|\mathbf{x}\|^2 \pm |x_1|\|\mathbf{x}\| \\ x_1 \in \mathbf{R} & \|\mathbf{x}\|^2 \pm x_1\|\mathbf{x}\| \end{cases}$$

$$\mathbf{u}^*\mathbf{u} = \overline{(x_1 \pm \mu x_1\|\mathbf{x}\|)}(x_1 \pm \mu x_1\|\mathbf{x}\|) + \sum_{i=2}^{n} \overline{x_i}x_i = (\overline{x_1} \pm \overline{\mu}x_1\|\mathbf{x}\|)(x_1 \pm \mu x_1\|\mathbf{x}\|) + \sum_{i=2}^{n} \overline{x_i}x_i =$$

$$= \overline{x_1}x_1 \pm \overline{\mu}x_1\|\mathbf{x}\| \pm \overline{x_1}\mu\|\mathbf{x}\| + \overline{\mu}\mu\|\mathbf{x}\|^2 + \sum_{i=2}^{n} \overline{x_i}x_i =$$

$$= \begin{cases} x_1 \in \mathbf{C} & \|\mathbf{x}\|^2 \pm 2\|\mathbf{x}\|\frac{\overline{x_1}x_1}{|x_1|} + |\mathbf{x}\|^2 = 2\|\mathbf{x}\|^2 \pm 2|x_1|\|\mathbf{x}\| = 2\mathbf{u}^*\mathbf{x} \\ x_1 \in \mathbf{R} & \|\mathbf{x}\|^2 \pm 2x_1\|\mathbf{x}\| + \|\mathbf{x}\|^2 = 2\mathbf{u}^*\mathbf{x} \end{cases}$$

Tedy $\mathbf{Rx} = \mathbf{x} - \mathbf{u} = \mp\mu\|\mathbf{x}\|\mathbf{e}_1$ □

Věta 9.10 *Pro každou matici* $\mathbf{A}$ *typu* $m \times n$ *nad* $\mathbf{C}^n$ *(nebo nad* $\mathbf{R}^n$*) existuje unitární (ortogonální) matice* $\mathbf{P}$ *řádu* m *taková, že* $\mathbf{PA} = \mathbf{T} = (t_{ij})$*, kde* $t_{ij} = 0$ *kdykoliv* $i > j$*.*

Důkaz. Dva důkazy, jeden pomocí Householderových reflektorů, druhý pomocí Givensových rotačních matic.
1. Householderův algoritmus
Označíme $\mathbf{x} = \mathbf{A}_{*1}$, zvolíme $\mathbf{u} = \mathbf{x} + \mu\|\mathbf{x}\|\mathbf{e}_1$ a $\mathbf{R}$ podle Tvrzení **??**.

$$\mathbf{RA} = \left(\begin{array}{c|ccc} \mu\|\mathbf{x}\| & * & \dots & * \\ \hline 0 & & & \\ \vdots & & \mathbf{A}_1 & \\ 0 & & & \end{array}\right)$$

$\mathbf{A}_1$ je typu $(m-1) \times (n-1)$. Najdeme $\mathbf{Q}_1$ takovou, že

$$\mathbf{Q}_1\mathbf{A}_1 = \left(\begin{array}{c|ccc} * & * & \dots & * \\ \hline 0 & & & \\ \vdots & & \mathbf{A}_2 & \\ 0 & & & \end{array}\right)$$

$\mathbf{Q}_1$ je čtvercová matice řádu $n-1$. Položíme

$$\mathbf{R}_1 = \left(\begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & \mathbf{Q}_1 & \\ 0 & & & \end{array}\right)$$

$$\mathbf{R}_1\mathbf{RA} = \mathbf{R}_1 \left(\begin{array}{c|ccc} \mu\|\mathbf{x}\| & * & \dots & * \\ \hline 0 & & & \\ \vdots & & \mathbf{A}_1 & \\ 0 & & & \end{array}\right) = \left(\begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & \mathbf{Q}_1 & \\ 0 & & & \end{array}\right) \left(\begin{array}{c|ccc} \mu\|\mathbf{x}\| & * & \dots & * \\ \hline 0 & & & \\ \vdots & & \mathbf{A}_1 & \\ 0 & & & \end{array}\right) =$$

$$= \left(\begin{array}{c|ccc} \mu\|\mathbf{x}\| & * & \dots & * \\ \hline 0 & & & \\ \vdots & & \mathbf{Q}_1\mathbf{A}_1 & \\ 0 & & & \end{array}\right) = \left(\begin{array}{cc|ccc} \mu\|\mathbf{x}\| & * & * & \dots & * \\ 0 & \mu_1\|\mathbf{x}_1\| & * & \dots & * \\ \hline 0 & 0 & & & \\ \vdots & \vdots & & \mathbf{A}_2 & \\ 0 & 0 & & & \end{array}\right)$$

Takto pokračujeme, dokud výsledná matice není horní trojúhelníková.
2. Givensův algoritmus
$\mathbf{x} = \mathbf{A}_{*1}$, pak $\mathbf{P}_{1n} \cdot \cdots \cdot \ldots \cdot \mathbf{P}_{12} \cdot \mathbf{x} = \|\mathbf{x}\|\mathbf{e}_1$

$$\mathbf{P}_{1n} \cdot \cdots \cdot \ldots \cdot \mathbf{P}_{12} \cdot \mathbf{A} = \left(\begin{array}{c|ccc} \|\mathbf{x}\| & * & \dots & * \\ \hline 0 & & & \\ \vdots & & \mathbf{A}_1 & \\ 0 & & & \end{array}\right)$$

Atd. □

Příklad 9.2 Výpočetní náročnost algoritmů použitých na regulární matici řádu n:

1. Gaussova eliminace $\approx \frac{1}{3}n^3$,
2. Gram-Schmidtova ortogonalizace $\approx n^3$,
3. Householderova redukce $\approx \frac{2}{3}n^3$,
4. Givensova redukce $\approx \frac{4}{3}n^3$.

Z uvedených algoritmů nejsou první dva numericky stabilní (i když Gaussovu eliminaci lze modifikovat tak, aby numericky stabilní byla pro většinu praktických problémů), zatímco poslední dva numericky stabilní jsou.

Algoritmus je považován za numericky stabilní, pokud dává přesné řešení blízké úlohy. Co se tím myslí, si ukážeme pomocí následujícího pojmu.

Definice 9.6 *Je-li* $\mathbf{A} = (a_{ij})$ *matice typu* $m \times n$ *nad* $\mathbf{C}$ *(*$\mathbf{R}$*), pak definujeme její* Frobeniovu normu *jako číslo*

$$\|\mathbf{A}\| = \sqrt{\sum_i \sum_j |a_{ij}|^2}.$$

Tvrzení 9.11 *Je-li* $\mathbf{A} = (a_{ij})$ *matice typu* $m \times n$ *nad* $\mathbf{C}$ *(*$\mathbf{R}$*) a* $\mathbf{Q}$ *unitární (ortogonální) matice řádu* m*, pak* $\|\mathbf{A}\| = \|\mathbf{QA}\|$.

Důkaz. Dle Věty **??** plati $\|\mathbf{Qx}\| = \|\mathbf{x}\|\ \forall \mathbf{x} \in \mathbf{C}^n(\mathbf{R}^n)$. Potom

$$\|\mathbf{QA}\|^2 = \sum_{j=1}^{n} \|\mathbf{QA}_{*j}\|^2 = \sum_{j=1}^{n} \|\mathbf{A}_{*j}\|^2 = \|\mathbf{A}\|^2$$

□

Budeme počítat QR-rozklad matice $\mathbf{A}$, tj. vyjádření $\mathbf{A} = \mathbf{QR}$, pomocí ortogonální redukce ma základě Věty **??**. Kvůli zaokrouhlovacím chybám nedostaneme přesně matice $\mathbf{Q}$ a $\mathbf{R}$, výsledky budou zatížené nějakou chybou, dostaneme $\mathbf{Q} + \mathbf{E}$ a $\mathbf{R} + \mathbf{F}$, kde $\mathbf{E}, \mathbf{F}$ jsou chybové matice zaokrouhlovacích chyb, které mají malou normu. Tyto matice jsou přesným QR-rozkladem matice

$$\tilde{\mathbf{A}} = (\mathbf{Q} + \mathbf{E})(\mathbf{R} + \mathbf{F}) = \mathbf{A} + \mathbf{QF} + \mathbf{RF} + \mathbf{EF}$$

Z těchto matic má $\mathbf{EF}$ zanedbatelnou normu, dále $\|\mathbf{QF}\| = \|\mathbf{F}\|$ podle Tvrzení **??** a $\|\mathbf{A}\| = \|\mathbf{QR}\| = \|\mathbf{R}\|$. Matice $\mathbf{QF}$ a $\mathbf{RE}$ proto neobsahují prvky s velkou hodnotou ve srovnání s prvky matice $\mathbf{A}$. Norma rozdílu $\tilde{\mathbf{A}} - \mathbf{A}$ je proto také malá ve srovnání s normou $\|\mathbf{A}\|$.

Kapitola 10

Ortogonální projekce a metoda nejmenších čtverců

V této kapitole budeme pracovat pouze nad tělesem reálných čísel.

Tvrzení 10.1 *Pro každou matici* $\mathbf{A}$ *typu* $m \times n$ *platí*

1. $r(\mathbf{A}^T\mathbf{A}) = r(\mathbf{A}\mathbf{A}^T) = r(\mathbf{A})$,
2. $\mathbf{S}(\mathbf{A}^T\mathbf{A}) = \mathbf{S}(\mathbf{A}^T)$,
3. $\mathbf{R}(\mathbf{A}^T\mathbf{A}) = \mathbf{R}(\mathbf{A})$,
4. $\mathbf{N}(\mathbf{A}^T\mathbf{A}) = \mathbf{N}(\mathbf{A})$,
5. $\mathbf{N}(\mathbf{A}\mathbf{A}^T) = \mathbf{N}(\mathbf{A}^T)$.

Důkaz.
1. Nechť $\{\mathbf{z}_1, \ldots, \mathbf{z}_k\}$ je báze $\mathbf{S}(\mathbf{A})$, ukážeme, že $\{\mathbf{A}^T\mathbf{x}_1, \ldots, \mathbf{A}^T\mathbf{x}_k\}$ tvoří bázi v $\mathbf{S}(\mathbf{A}^T\mathbf{A})$. Víme, že $\mathbf{S}(\mathbf{A}^T\mathbf{A}) \subseteq \mathbf{S}(\mathbf{A}^T)$, tedy $r(\mathbf{A}^T\mathbf{A}) \leq r(\mathbf{A}^T) = r(\mathbf{A})$. Stačí dokázat, že $\{\mathbf{A}^T\mathbf{x}_1, \ldots, \mathbf{A}^T\mathbf{z}_k\}$ je lineárně nezávislá (pak bude maximální lineárně nezávislá množina a tedy báze). Odtud vyplyne, že $r(\mathbf{A}^T\mathbf{A}) \geq r(\mathbf{A})$. Je-li

$$\sum_{i=1}^{k} a_i \mathbf{A}^T\mathbf{z}_i = \mathbf{0}$$

, pak platí:

$$\sum_{i=1}^{k} \mathbf{A}^T(a_i\mathbf{z}_i) = \mathbf{0} = \mathbf{A}^T \cdot \sum_{i=1}^{k}(a_i\mathbf{z}_i)$$

Označíme

$$\mathbf{y} = \sum_{i=1}^{k} (a_i \mathbf{z}_i)$$

$\mathbf{A}^T\mathbf{y} = \mathbf{0}$, tj. $\mathbf{y} \in \mathbf{N}(\mathbf{A}^T)$, $\mathbf{y}$ je lineární kombinací $\mathbf{z}_i \in \mathbf{S}(\mathbf{A})$, tedy $\mathbf{y} \in \mathbf{S}(\mathbf{A})$, tj. existuje $\mathbf{x} \in \mathbf{T}^n$ takový, že $\mathbf{y} = \mathbf{A}\mathbf{x}$. Spočítáme $\mathbf{y}^T\mathbf{y} = (\mathbf{A}\mathbf{x})^T\mathbf{y} = \mathbf{x}^T\mathbf{A}^T\mathbf{y} = \mathbf{0}$, tj. $\|\mathbf{y}\| = 0 \Leftrightarrow \mathbf{y} = \mathbf{0}$. Víme tedy, že

$$\sum_{i=1}^{k} a_i \mathbf{z}_i = \mathbf{0} \overset{*}{\Leftrightarrow} a_i = 0 \quad \forall i = 1, \ldots, k$$

Poznámka: * - protože $\{\mathbf{z}_1, \ldots, \mathbf{z}_k\}$ je lineárně nezávislá Tedy $r(\mathbf{A}^T\mathbf{A}) \leq k = \dim \mathbf{S}(\mathbf{A}) = r(\mathbf{A})$.
Položíme $\mathbf{B} = \mathbf{A}^T$, právě jsme dokázali, že $r(\mathbf{B}^T\mathbf{B}) = r(\mathbf{B})$, po dosazení $r(\mathbf{A}\mathbf{A}^T) = r(\mathbf{A}^T) = r(\mathbf{A})$.
2. Víme, že $\mathbf{S}(\mathbf{A}^T\mathbf{A}) \subseteq \mathbf{S}(\mathbf{A}^T)$ a $\dim \mathbf{S}(\mathbf{A}^T\mathbf{A}) = r(\mathbf{A}^T\mathbf{A}) = r(\mathbf{A}) = r(\mathbf{A}^T) = \dim \mathbf{S}(\mathbf{A}^T)$
3. Plyne z 2, položíme-li $\mathbf{B} = \mathbf{A}^T$.
4.$\mathbf{N}(\mathbf{A}) \subseteq \mathbf{N}(\mathbf{A}^T\mathbf{A})$, $\dim \mathbf{N}(\mathbf{A}) = n - \dim \mathbf{S}(\mathbf{A}) = n - r(\mathbf{A}) = n - r(\mathbf{A}^T\mathbf{A}) = n - \dim \mathbf{S}(\mathbf{A}^T\mathbf{A}) = \dim \mathbf{N}(\mathbf{A}^T\mathbf{A})$.
5. Plyne ze 4, položíme-li $\mathbf{B} = \mathbf{A}^T$. □

Tvrzení 10.2 *Buď $\mathbf{A}\mathbf{x} = \mathbf{b}$ soustava m lineárních rovnic o n neznámých. Pak*

1. *soustava $\mathbf{A}^T\mathbf{A}\mathbf{x} = \mathbf{A}^T\mathbf{b}$ je vždy řešitelná,*

2. *je-li $\mathbf{A}\mathbf{x} = \mathbf{b}$ řešitelná, pak množina všech řešení soustavy $\mathbf{A}\mathbf{x} = \mathbf{b}$ se rovná množině všech řešení soustavy $\mathbf{A}^T\mathbf{A}\mathbf{x} = \mathbf{A}^T\mathbf{b}$,*

3. *soustava $\mathbf{A}^T\mathbf{A}\mathbf{x} = \mathbf{A}^T\mathbf{b}$ má jednoznačné řešení právě tehdy když $r(\mathbf{A}) = n$, v takovém případě pak $\mathbf{x} = (\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{b}$.*

Důkaz.
1. $\mathbf{A}^T\mathbf{b} \in \mathbf{S}(\mathbf{A}^T) \in \mathbf{S}(\mathbf{A}^T\mathbf{A}) \Rightarrow \mathbf{A}^T\mathbf{A}\mathbf{x} = \mathbf{A}^T\mathbf{b}$ má řešeí $\forall \mathbf{b}$.
2. Násobení rovnice maticí $\mathbf{A}^T$ zleva není ekvivalentní úprava. Je-li $\mathbf{z}$ řešením $\mathbf{A}\mathbf{x} = \mathbf{b} \Rightarrow \mathbf{A}^T\mathbf{A}\mathbf{z} = \mathbf{A}^T\mathbf{b}$ tedy $\mathbf{z}$ je řešením (asociované) soustavy $\mathbf{A}^T\mathbf{A}\mathbf{x} = \mathbf{A}^T\mathbf{b}$. Množina všech řešení $\mathbf{A}\mathbf{x} = \mathbf{b}$ se rovná $\mathbf{z} + \mathbf{N}(\mathbf{A}) = \mathbf{z} + \mathbf{N}(\mathbf{A}^T\mathbf{A})$, což je množina všech řešení asociované soustavy.
3. $\mathbf{A}^T\mathbf{A}\mathbf{x} = \mathbf{A}^T\mathbf{b}$ má jednoznačné řešení $\Leftrightarrow \mathbf{N}(\mathbf{A}^T\mathbf{A}) = \{\mathbf{0}\} \overset{10.1.4}{\Leftrightarrow} \mathbf{N}(\mathbf{A}) =$

$\{\mathbf{0}\} \Leftrightarrow \dim \mathbf{N}(\mathbf{A}) = 0 \overset{\dim \mathbf{N}(\mathbf{A})+r(\mathbf{A})=n}{\Leftrightarrow} r(\mathbf{A}) = n.$
Pokud $r(\mathbf{A}) = n \Rightarrow r(\mathbf{A}^T\mathbf{A}) = n \Leftrightarrow \mathbf{A}^T\mathbf{A}$ je regulární. □

Ve Větě **??** si ukážeme, že v případě neřešitelné soustavy rovnic $\mathbf{Ax} = \mathbf{b}$ každé řešení $\mathbf{x}$ soustavy $\mathbf{A}^T\mathbf{Ax} = \mathbf{A}^T\mathbf{b}$ minimalizuje normu $\|\mathbf{Ax} - \mathbf{b}\|$. Jinak řečeno, v případě neřešitelné soustavy $\mathbf{Ax} = \mathbf{b}$ je vektor $\mathbf{Ax}$ nejblíže vektoru pravých stran $\mathbf{b}$ právě pro ty vektory $\mathbf{x}$, které jsou řešením soustavy $\mathbf{A}^T\mathbf{Ax} = \mathbf{A}^T\mathbf{b}$.

Definice 10.1 *Je-li* $\mathbf{Ax} = \mathbf{b}$ *soustava lineárních rovnic, pak soustavu* $\mathbf{A}^T\mathbf{Ax} = \mathbf{A}^T\mathbf{b}$ *nazýváme* asociovaný systém normálních rovnic *k soustavě* $\mathbf{Ax} = \mathbf{b}$.

Příklad 10.1 Výpočet dráhy rakety.

Příklad 10.2 Známe-li QR-rozklad $\mathbf{A} = \mathbf{QR}$ matice $\mathbf{A}$ s lineárně nezávislými sloupci, můžeme jej použít k řešení soustavy $\mathbf{A}^T\mathbf{Ax} = \mathbf{A}^T\mathbf{b}$. Připomeňme si, že sloupce $\mathbf{Q}$ tvoří ortonormální množinu a $\mathbf{R}$ je horní trojúhelníková matice s kladnými prvky na hlavní diagonále. Potom platí

$$\mathbf{A}^T\mathbf{A} = \mathbf{R}^T\mathbf{Q}^T\mathbf{QR} = \mathbf{R}^T\mathbf{R}.$$

Protože $\mathbf{Q}$ má ortonormální sloupce, platí $\mathbf{Q}^T\mathbf{Q} = \mathbf{I}$ a soustava $\mathbf{A}^T\mathbf{Ax} = \mathbf{A}^T\mathbf{b}$ je tak ekvivalentní soustavě $\mathbf{R}^T\mathbf{Rx} = \mathbf{R}^T\mathbf{Q}^T\mathbf{b}$. Matice $\mathbf{R}^T$ je regulární, takže tato soustava je dále ekvivalentní soustavě $\mathbf{Rx} = \mathbf{Q}^T\mathbf{b}$, kterou můžeme vyřešit zpětnou substitucí a dostaneme tak jediné řešení $\mathbf{x} = \mathbf{R}^{-1}\mathbf{Q}^T\mathbf{b}$ soustavy $\mathbf{A}^T\mathbf{Ax} = \mathbf{A}^T\mathbf{b}$.

Věta 10.3 Věta o ortogonálním rozkladu. $\mathbf{A}$ *typu* $m \times n$ *nad* $\mathbf{R}$ *platí*

1. $\mathbf{S}(\mathbf{A})^\perp = \mathbf{N}(\mathbf{A}^T)$,
2. $\mathbf{N}(\mathbf{A})^\perp = \mathbf{S}(\mathbf{A}^T)$.

Důkaz.
1. $\mathbf{x} \in \mathbf{S}(\mathbf{A})^\perp \Leftrightarrow (\forall \mathbf{y} \in \mathbf{R}^n) : (< \mathbf{Ay}, \mathbf{x} >= 0) \Leftrightarrow (\forall \mathbf{y} \in \mathbf{R}^n)(\mathbf{y}^T\mathbf{A}^T\mathbf{x} = 0) \Leftrightarrow (\forall \mathbf{y} \in \mathbf{R}^n)(< \mathbf{y}, \mathbf{A}^T\mathbf{x} >= 0) \Leftrightarrow \ldots$
Označíme $\mathbf{S}(\mathbf{A}) = \{\mathbf{Ay}, \mathbf{y} \in \mathbf{R}^n\}$.
$\ldots \Leftrightarrow \mathbf{A}^T\mathbf{x} \in (\mathbf{R}^n)^\perp \Leftrightarrow \mathbf{A}^T\mathbf{x} = \mathbf{0} \Leftrightarrow \mathbf{x} \in \mathbf{N}(\mathbf{A}^T)$
2. Použijeme 1. na matici $\mathbf{B} = \mathbf{A}|T$.
$\mathbf{S}(\mathbf{B})^\perp = \mathbf{N}(\mathbf{B}^T) = \mathbf{N}(\mathbf{A})$
$\mathbf{S}(\mathbf{A}^T) = (\mathbf{S}(\mathbf{A}^T)^\perp)^\perp = \mathbf{N}(\mathbf{A})^\perp$ □

Důsledek 10.4 Fredholmova alternativa. *Pro každou matici* $\mathbf{A}$ *nastává právě jedna z následujících dvou možností:*

1. *soustava* $\mathbf{Ax} = \mathbf{b}$ *má řešení pro každou pravou stranu* $\mathbf{b}$,
2. *soustava* $\mathbf{A}^T\mathbf{y} = \mathbf{0}$ *má nenulové řešení.*

Důkaz. Plyne z Věty **??**.1. $\mathbf{A}$ je typu $m \times n$.
1. $\mathbf{Ax} = \mathbf{b}$ má vždy řešení $\Leftrightarrow \mathbf{S}(\mathbf{A}) = \mathbf{R}^m \Leftrightarrow \mathbf{N}(\mathbf{A}^T) = \{\mathbf{0}\} \Leftrightarrow \mathbf{A}^T\mathbf{y} = \mathbf{0}$ má pouze nulové řešení.
2. $\mathbf{A}^T\mathbf{y} = \mathbf{0}$ má nenulové řešení $\Leftrightarrow \mathbf{N}(\mathbf{A}^T) \neq \{\mathbf{0}\} \Leftrightarrow \mathbf{S}(\mathbf{A})^\perp \neq \{\mathbf{0}\} \Leftrightarrow \mathbf{S}(\mathbf{A}) \neq \{\mathbf{0}\}^\perp = \mathbf{R}^m \Leftrightarrow \mathbf{Ax} = \mathbf{b}$ nemá vždy řešešní. □

Tvrzení 10.5 *Buď* $\mathbf{A}$ *matice typu* $m \times n$ *nad* $\mathbf{R}$ *a* $r(\mathbf{A}) = r$. *Pak existují ortogonální matice* $\mathbf{U}$ *řádu* m, *ortogonální matice* $\mathbf{V}$ *řádu* n *a regulární matice* $\mathbf{C}$ *řádu* r *takové, že*

$$\mathbf{A} = \mathbf{U} \begin{pmatrix} \mathbf{C} & \mathbf{0}_{r\times(n-r)} \\ \mathbf{0}_{(m-r)\times r} & \mathbf{0}_{(m-r)\times(n-r)} \end{pmatrix} \mathbf{V}^T.$$

Prvních r *sloupců matice* $\mathbf{U}$ *tvoří ortonormální bázi* $\mathbf{S}(\mathbf{A})$, *posledních* $m-r$ *sloupců tvoří ortonormální bázi* $\mathbf{N}(\mathbf{A}^T)$. *Prvních* r *sloupců* $\mathbf{V}$ *tvoří ortonormální bázi* $\mathbf{S}(\mathbf{A}^T)$ *a posledních* $n-r$ *sloupců tvoří ortonormální bázi* $\mathbf{N}(\mathbf{A})$.

Důkaz. Zvolíme ortonormální bázi $\{\mathbf{u}_1, \ldots, \mathbf{u}_r\}$ v $\mathbf{S}(\mathbf{A})$ a bázi $\{\mathbf{u}_{r+1}, \ldots, \mathbf{u}_m\}$ v $\mathbf{N}(\mathbf{A}^T) = \mathbf{S}(\mathbf{A})^\perp$. Tedy $\mathbf{U} = (\mathbf{u}_1|\ldots|\mathbf{u}_m)$ je ortogonální.
$\mathbf{V} = (\mathbf{v}_1|\ldots|\mathbf{v}_n)$, $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ je ortonormální báze v $\mathbf{S}(\mathbf{A}^T)$, $\{\mathbf{v}_{r+1}, \ldots, \mathbf{v}_n\}$ je ortonormální báze v $\mathbf{N}(\mathbf{A}) = \mathbf{S}(\mathbf{A}^T)^\perp$.
$\mathbf{U}^T\mathbf{AV} = (r_{ij})$ je typu $m \times n$.
$\mathbf{A}^T\mathbf{u}_i = \mathbf{0} \quad \forall i = (r+1), \ldots, m$
$\mathbf{u}_i^T\mathbf{A} = \mathbf{0} \quad \forall i = (r+1), \ldots, m$
$\mathbf{Av}_j = \mathbf{0} \quad \forall j = (r+1), \ldots, n$
$r_{ij} = \mathbf{u}_i^T\mathbf{Av}_j$
$r_{ij} = 0 \quad \forall i > r$
$r_{ij} = 0 \quad \forall j > r$

$$\mathbf{R} = \mathbf{U}^T\mathbf{AV} = \left(\begin{array}{c|c} \mathbf{C} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} \end{array}\right)$$

Zbývá dokázat, že $\mathbf{C}$ je regulární. Platí, že: $r(\mathbf{C}) = r(\mathbf{R}) = r(\mathbf{U}^T\mathbf{AV}) = r(\mathbf{AU}^T) = r(\mathbf{A}) = r$. Poznámka: $\mathbf{U}^T, \mathbf{V}$ jsou regulární - tedy lze je rozložit na součín elementárních matic. □

Definice 10.2 *Buď* $\mathbf{A}$ *matice typu* $m \times n$ *nad* $\mathbf{R}$ *a* $r(\mathbf{A}) = r$. *Vyjádření* $\mathbf{A} = \mathbf{URV}^T$, *kde* $\mathbf{U}$ *je ortogonální matice řádu* m, $\mathbf{V}$ *je ortogonální matice řádu* n *a*

$$\mathbf{R} = \begin{pmatrix} \mathbf{C} & \mathbf{0}_{r\times(n-r)} \\ \mathbf{0}_{(m-r)\times r} & \mathbf{0}_{(m-r)\times(n-r)} \end{pmatrix}$$

je matice typu $m\times n$, *a* $\mathbf{C}$ *je regulární matice řádu* r, *se nazývá* URV-rozklad matice $\mathbf{A}$.

Všimněte si, že URV-rozklad matice $\mathbf{A}$ není určený jednoznačně.

Tvrzení 10.6 *Buď* $\mathbf{A} = \mathbf{URV}^T$ *URV-rozklad matice* $\mathbf{A}$. *Matice*

$$\mathbf{B} = \mathbf{V}\begin{pmatrix} \mathbf{C}^{-1} & \mathbf{0}_{r\times(m-r)} \\ \mathbf{0}_{(n-r)\times r} & \mathbf{0}_{(n-r)\times(m-r)} \end{pmatrix}\mathbf{U}^T,$$

splňuje následující rovnosti

1. $\mathbf{ABA} = \mathbf{A}$,
2. $\mathbf{BAB} = \mathbf{B}$,
3. $(\mathbf{AB})^T = \mathbf{AB}$,
4. $(\mathbf{BA})^T = \mathbf{BA}$.

Matice $\mathbf{B}$ *je těmito čtyřmi rovnostmi určena jednoznačně.*

Důkaz. 1.

$$\mathbf{ABA} = \mathbf{URV}^T\mathbf{V}\begin{pmatrix} \mathbf{C}^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}\mathbf{U}^T\mathbf{URV}^T = \mathbf{U}\begin{pmatrix} \mathbf{C} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}\begin{pmatrix} \mathbf{C}^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}\begin{pmatrix} \mathbf{C} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}\mathbf{V}^T = \ldots$$

$$\ldots = \mathbf{U}\begin{pmatrix} \mathbf{I}_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}\begin{pmatrix} \mathbf{C} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}\mathbf{V}^T = \mathbf{A}$$

2. analogicky

3.

$$\mathbf{AB} = \mathbf{U}\begin{pmatrix} \mathbf{C} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}\mathbf{V}^T\mathbf{V}\begin{pmatrix} \mathbf{C}^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}\mathbf{U}^T = \mathbf{U}\begin{pmatrix} \mathbf{I}_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}\mathbf{U}^T$$

$$(\mathbf{AB})^T = \left(\mathbf{U}\begin{pmatrix} \mathbf{I}_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}\mathbf{U}^T\right)^T = (\mathbf{U}^T)^T\left(\mathbf{U}\begin{pmatrix} \mathbf{I}_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}\right)^T = \mathbf{U}\begin{pmatrix} \mathbf{I}_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}\mathbf{U}^T = \mathbf{AB}$$

4. analogicky
Jednoznačnost: $\mathbf{AC} = (\mathbf{AC})^T = \mathbf{C}^T\mathbf{A}^T = \mathbf{C}^T(\mathbf{ABA})^T = \mathbf{C}^T\mathbf{B}^T\mathbf{A}^T = (\mathbf{AC})^T(\mathbf{AB})^T = \mathbf{ACAB} \overset{\mathbf{ACA=A}}{=} \mathbf{AB}$, stejně se dokáže, že $\mathbf{CA} = \mathbf{BA}$, potom $\mathbf{B} = \mathbf{BAB} = \mathbf{BAC} = \mathbf{CAC} = \mathbf{C}$. □

Definice 10.3 *Buď* $\mathbf{A}$ *matice typu* $m \times n$ *nad* $\mathbf{R}$. *Matici* $\mathbf{B}$ *splňující rovnosti 1,2,3,4 z Tvrzení* **??** *nazýváme* Moore-Penroseova inverze *nebo také* pseudoinverze *matice* $\mathbf{A}$ *a označujeme ji* $\mathbf{A}^{\dagger}$.

Tvrzení 10.7 *Buď* $\mathbf{M}$ *podprostor* $\mathbf{R}^n$ *a* $\mathbf{M}^{\perp}$ *jeho ortogonální doplněk. Potom každý vektor* $\mathbf{x} \in \mathbf{R}^n$ *lze vyjádřit právě jedním způsobem ve tvaru* $\mathbf{x} = \mathbf{p} + \mathbf{q}$, *kde* $\mathbf{p} \in \mathbf{M}$ *a* $\mathbf{q} \in \mathbf{M}^{\perp}$.

Důkaz. Zvolíme $\{\mathbf{u}_1, \ldots, \mathbf{u}_r\}$ ortonormální bázi v $\mathbf{M}$ a $\{\mathbf{u}_{r+1}, \ldots, \mathbf{u}_n\}$ ortonormální bázi v $\mathbf{M}^{\perp}$. Pak $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ je ortonormální báze v $\mathbf{R}^n$. Pak

$$\mathbf{x} = \sum_{i=1}^{n} a_i \mathbf{u}_i$$

$$\sum_{i=1}^{r} a_i \mathbf{u}_i = \mathbf{p} \in \mathbf{M}$$

$$\sum_{i=r+1}^{b} a_i \mathbf{u}_i = \mathbf{q} \in \mathbf{M}^{\perp}$$

Jednoznačnost: je-li $\mathbf{x} = \mathbf{p} + \mathbf{q} = \mathbf{p}' + \mathbf{q}'$, kde $\mathbf{p}, \mathbf{p}' \in \mathbf{M}$, $\mathbf{q}, \mathbf{q}' \in \mathbf{M}^{\perp}$, potom
$\mathbf{p} + \mathbf{q} = \mathbf{p}' + \mathbf{q}'$
$\mathbf{p} - \mathbf{p}' = \mathbf{q}' - \mathbf{q}$;
$\mathbf{p} - \mathbf{p}' \in \mathbf{M}$, $\mathbf{q}' - \mathbf{q} \in \mathbf{M}^{\perp} \Leftrightarrow \mathbf{p} - \mathbf{p}' = \mathbf{0} = \mathbf{q}' - \mathbf{q}$, protože $\mathbf{M} \cap \mathbf{M}^{\perp} = \{\mathbf{0}\}$.
□

Definice 10.4 *Je-li* $\mathbf{M}$ *podprostor* $\mathbf{R}^n$ *a* $\mathbf{x} = \mathbf{p} + \mathbf{q}$, *kde* $\mathbf{p} \in \mathbf{M}$ *a* $\mathbf{q} \in \mathbf{M}^{\perp}$, *pak vektor* $\mathbf{p}$ *nazýváme* ortogonální projekce $\mathbf{x}$ *na podprostor* $\mathbf{M}$.

Tvrzení 10.8 *Buď* $\mathbf{M}$ *podprostor* $\mathbf{R}^n$, $\mathbf{x} \in \mathbf{R}^n$ *a* $\mathbf{p} \in \mathbf{M}$ *ortogonální projekce vektoru* $\mathbf{x}$ *na* $\mathbf{M}$. *Pak pro každý vektor* $\mathbf{m} \in \mathbf{M}$ *platí*

$$\|\mathbf{x} - \mathbf{p}\| \leq \|\mathbf{x} - \mathbf{m}\|,$$

přičemž rovnost nastává právě když $\mathbf{m} = \mathbf{p}$.

Důkaz. Pro $\mathbf{m} = \mathbf{p}$ tvrzení platí triviálně. Je-li $\mathbf{m} \neq \mathbf{p}$, potom
$\mathbf{x} - \mathbf{m} = (\mathbf{x} - \mathbf{p}) + (\mathbf{p} - \mathbf{m})$, $\mathbf{x} - \mathbf{p} = \mathbf{q} \in \mathbf{M}^{\perp}$, $(\mathbf{p} - \mathbf{m}) \in \mathbf{M}$.
$(\mathbf{x} - \mathbf{p}) \perp (\mathbf{p} - \mathbf{m}) \Rightarrow \|\mathbf{x} - \mathbf{m}\|^2 = \|\mathbf{x} - \mathbf{p}\|^2 + \|\mathbf{p} - \mathbf{m}\|^2 > \|\mathbf{x} - \mathbf{p}\|^2$. □

Tvrzení 10.9 *Buď* $\mathbf{A}$ *matice typu* $m \times n$ *a* $\mathbf{A}^\dagger$ *Moore-Penroseova inverze* $\mathbf{A}$. *Potom se ortogonální projekce libovolného vektoru* $\mathbf{b} \in \mathbf{R}^m$ *na sloupcový prostor* $\mathbf{S}(\mathbf{A})$ *matice* $\mathbf{A}$ *rovná* $(\mathbf{A}\mathbf{A}^\dagger)\mathbf{b}$.

Důkaz. Je-li $\mathbf{P} = \mathbf{A}\mathbf{A}^\dagger$, pak platí $\mathbf{P}^2 = \mathbf{A}\mathbf{A}^\dagger\mathbf{A}\mathbf{A}^\dagger = \mathbf{A}\mathbf{A}^\dagger = \mathbf{P}$,
$\mathbf{P}\mathbf{A} = \mathbf{A}\mathbf{A}^\dagger\mathbf{A} = \mathbf{A}$.
Ukážeme, že $\mathbf{S}(\mathbf{A}) = \{\mathbf{y}; \mathbf{y} \in \mathbf{R}^m, \mathbf{P}\mathbf{y} = \mathbf{y}\}$.
1. '$\subseteq$': Je-li $\mathbf{y} \in \mathbf{S}(\mathbf{A})$, pak $\mathbf{y} = \mathbf{A}\mathbf{b}$ pro nějaké $\mathbf{b} \in \mathbf{R}^n$ a $\mathbf{P}\mathbf{y} = \mathbf{P}\mathbf{A}\mathbf{b} = \mathbf{A}\mathbf{b} = \mathbf{y}$.
2. '$\supseteq$': Je-li naopak $\mathbf{P}\mathbf{y} = \mathbf{y}$, tj. $\mathbf{y} = \mathbf{A}(\mathbf{A}^\dagger\mathbf{y}) \in \mathbf{S}(\mathbf{A})$, zvolme $\mathbf{b} \in \mathbf{R}^n$.
$\mathbf{b} = \mathbf{P}\mathbf{b} + (\mathbf{b} - \mathbf{P}\mathbf{b}) = \mathbf{P}\mathbf{b} + (\mathbf{I}_n - \mathbf{P})\mathbf{b}$
Chceme ukázat, že $(\mathbf{I}_n - \mathbf{P})\mathbf{b} \in \mathbf{S}(\mathbf{A})^\perp$. Víme, že $\mathbf{P}\mathbf{y} = \mathbf{y} \in \mathbf{S}(\mathbf{A})$.
$< \mathbf{y}, (\mathbf{I}_n - \mathbf{P})\mathbf{b} >= \mathbf{y}^T(\mathbf{I}_n - \mathbf{P})\mathbf{b} = (\mathbf{P}\mathbf{y})^T(\mathbf{I}_n - \mathbf{P})\mathbf{b} = \mathbf{y}^T\mathbf{P}^T(\mathbf{I}_n - \mathbf{P})\mathbf{b} = \mathbf{y}^T\mathbf{P}(\mathbf{I}_n - \mathbf{P})\mathbf{b} = \mathbf{y}^T(\mathbf{P} - \mathbf{P}^2)\mathbf{b} = 0$.
Z vyjádření $\mathbf{b} = \mathbf{P}\mathbf{b} + (\mathbf{b} - \mathbf{P}\mathbf{b})$, kde $(\mathbf{b} - \mathbf{P}\mathbf{b}) \in \mathbf{S}(\mathbf{A})^\perp$, plyne, že $\mathbf{P}\mathbf{b} \in \mathbf{S}(\mathbf{A})$, tedy $\mathbf{P}\mathbf{b}$ je ortogonální projekce $\mathbf{b}$ na $\mathbf{S}(\mathbf{A})$. □

Věta 10.10 Metoda nejmenších čtverců *Nechť* $\mathbf{A}\mathbf{x} = \mathbf{b}$ *je soustava lineárních rovnic nad* $\mathbf{R}$. *Pak pro vektor* $\mathbf{x} \in \mathbf{R}^n$ *je ekvivalentní*

1. $\mathbf{A}^T\mathbf{A}\mathbf{x} = \mathbf{A}^T\mathbf{b}$,
2. $\mathbf{A}\mathbf{x} = (\mathbf{A}\mathbf{A}^\dagger)\mathbf{b}$.

Důkaz. Označme $\mathbf{P} = \mathbf{A}\mathbf{A}^\dagger$. $\forall \mathbf{x} \in \mathbf{R}^n$ platí $\mathbf{A}\mathbf{x} \in \mathbf{S}(\mathbf{A})$, tj. $\mathbf{P}\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}$.
Platí i $\mathbf{A}\mathbf{x} = \mathbf{P}\mathbf{b} \Leftrightarrow \mathbf{P}\mathbf{A}\mathbf{x} = \mathbf{P}\mathbf{b} \Leftrightarrow \mathbf{P}(\mathbf{A}\mathbf{x} - \mathbf{b}) = 0 \Leftrightarrow \mathbf{A}\mathbf{x} - \mathbf{b} \in \mathbf{N}(\mathbf{P}) = \mathbf{S}(\mathbf{P}^T)^\perp = \mathbf{S}(\mathbf{P})^\perp = \mathbf{S}(\mathbf{A})^\perp = \mathbf{N}(\mathbf{A}^T) \Leftrightarrow \mathbf{A}^T(\mathbf{A}\mathbf{x} - \mathbf{b}) = 0 \Leftrightarrow \mathbf{A}^T\mathbf{A}\mathbf{x} = \mathbf{A}^T\mathbf{b}$.
Poznámka: Víme, že $\mathbf{S}(\mathbf{P}) \subseteq \mathbf{S}(\mathbf{A})$, z $\mathbf{S}(\mathbf{A}) = \{\mathbf{y}; \mathbf{y} \in \mathbf{R}^m, \mathbf{P}\mathbf{y} = \mathbf{y}\}$ vyplývá, že $\mathbf{S}(\mathbf{A}) \subseteq \mathbf{S}(\mathbf{P})$, tedy $\mathbf{S}(\mathbf{A}) = \mathbf{S}(\mathbf{P})$. □

Kapitola 11

Matice jako lineární zobrazení

V této kapitole budeme pracovat nad obecným tělesem $\mathbf{T}$.

Definice 11.1 *Buď* $\mathbf{A}$ *matice typu* $m \times n$ *nad tělesem* $\mathbf{T}$. *Zobrazení* $A : \mathbf{T}^n \to \mathbf{T}^m$ *definované předpisem* $A(\mathbf{x}) = \mathbf{Ax}$ *nazýváme* lineární zobrazení určené maticí $\mathbf{A}$.

Tvrzení 11.1 *Je-li* $A : \mathbf{T}^n \to \mathbf{T}^m$ *lineární zobrazení určené maticí* $\mathbf{A}$, *pak platí*

1. $A(\mathbf{x}+\mathbf{y}) = A(\mathbf{x}) + A(\mathbf{y})$ *pro každé* $\mathbf{x}, \mathbf{y} \in \mathbf{T}^n$,
2. $A(a\mathbf{x}) = a \cdot A(\mathbf{x})$ *pro každý vektor* $\mathbf{x} \in \mathbf{T}^n$ *a každý skalár* $a \in \mathbf{T}$.

Důkaz.
1. $A(\mathbf{x}+\mathbf{y}) = \mathbf{A}(\mathbf{x}+\mathbf{y}) = \mathbf{Ax} + \mathbf{Ay} = A(\mathbf{x}) + A(\mathbf{y})$
2. $A(a\mathbf{x}) = \mathbf{A}a\mathbf{x} = a\mathbf{Ax} = a \cdot A(\mathbf{x})$ □

Definice 11.2 *Libovolné zobrazení* $A : \mathbf{T}^n \to \mathbf{T}^m$ *splňující podmínky 1,2 Tvrzení* **??** *nazýváme* lineární zobrazení.

Tvrzení 11.2 *Každé lineární zobrazení* $A : \mathbf{T}^n \to \mathbf{T}^m$ *je určené nějakou maticí.*

Důkaz. Vezmeme standardní bázi $\mathbf{e}_1, \ldots, \mathbf{e}_n \in \mathbf{T}^n$. Označíme

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_{\mathbf{e}_1} & \mathbf{A}_{\mathbf{e}_2} & \ldots & \mathbf{A}_{\mathbf{e}_n} \end{pmatrix}$$

$\mathbf{A}\mathbf{e}_i = A(\mathbf{e}_i)$. Je-li $\mathbf{x} = (x_1, \ldots, x_n)^T \in \mathbf{T}^n$, pak

$$\mathbf{x} = \sum_{i=1}^{n} x_i \mathbf{e}_i$$

$$A(\mathbf{x}) = A\left(\sum_{i=1}^{n} x_i \mathbf{e}_i\right) = \sum_{i=1}^{n} x_i A(\mathbf{e}_i) = \sum_{i=1}^{n} x_i \mathbf{A}\mathbf{e}_i = \mathbf{A}\left(\sum_{i=1}^{n} x_i \mathbf{e}_i\right) = \mathbf{A}\mathbf{x} \in \mathbf{T}^n$$

□

Tvrzení 11.3 *Buď* $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ *báze* $\mathbf{T}^n$ *a* $\mathbf{x} \in \mathbf{T}^n$. *Jsou-li* $\mathbf{x} = \sum_{i=1}^{n} a_i \mathbf{u}_i$ *a* $\mathbf{x} = \sum_{i=1}^{n} b_i \mathbf{u}_i$ *dvě vyjádření* $\mathbf{x}$ *jako lineární kombinace prvků báze* $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$, *pak* $a_i = b_i$ *pro každé* $i = 1, 2, \ldots, n$.

Důkaz. Z předpokladů plyne:

$$\sum_{i=1}^{n} (a_i - b_i)\mathbf{u}_i = \mathbf{0}$$

$\mathbf{u}_1, \ldots, \mathbf{u}_n$ je lineárně nezávislá $\rightarrow a_i - b_i = 0 \ \forall i = 1, \ldots, n$. □

Definice 11.3 *Je-li* $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ *báze* $\mathbf{T}^n$ *a* $\mathbf{x} = \sum_{i=1}^{n} a_i \mathbf{u}_i$, *pak aritmetický vektor* $(a_1, \ldots, a_n)^T \in \mathbf{T}^n$ *nazýváme* vektor souřadnic *vektoru* $\mathbf{x}$ vzhledem k bázi $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$, *nebo stručněji* souřadnice vektoru $\mathbf{x}$ vzhledem k bázi $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$.

Poznámka Je-li $\mathbf{x} = (x_1, \ldots, x_n)^T \in \mathbf{T}^n$, pak $x_1, \ldots, x_n$ jsou souřadnice vektoru $\mathbf{x}$ vzhledem ke standardní bázi $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$, neboť $\mathbf{x} = \sum_{i=1}^{n} x_i \mathbf{e}_i$. V další části přednášky už nebudeme standardní bázi tolik upřednostňovat a budeme se zabývat souřadnicemi vektorů vzhledem k obecným bázím.

Tvrzení 11.4 *Předpokládejme, že* $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ *a* $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ *jsou dvě báze prostoru* $\mathbf{T}^n$. *Nechť pro nějaký vektor* $\mathbf{x} \in \mathbf{T}^n$ *platí*

$$\mathbf{x} = \sum_{i=1}^{n} a_i \mathbf{u}_i = \sum_{i=1}^{n} b_i \mathbf{v}_i,$$

tj. $a_1, \ldots, a_n$ *jsou souřadnice* $\mathbf{x}$ *vzhledem k bázi* $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ *a* $b_1, \ldots, b_n$ *jsou souřadnice téhož vektoru* $\mathbf{x}$ *vzhledem k bázi* $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$.

Nechť

$$\mathbf{v}_j = \sum_{i=1}^{n} p_{ij}\mathbf{u}_i$$

pro každé $j = 1, \ldots, n$. *Označme* $\mathbf{P} = (p_{ij})$. *Potom platí*

$$(a_1, \ldots, a_n)^T = \mathbf{P}(b_1, \ldots, b_n)^T.$$

Důkaz.

$$\mathbf{x} = \sum_{j=1}^{n} b_j\mathbf{v}_j = \sum_{j=1}^{n} b_j \left(\sum_{i=1}^{n} p_{ij}\mathbf{u}_i\right) = \sum_{j=1}^{n}\sum_{i=1}^{n} b_j p_{ij}\mathbf{u}_i = \sum_{i=1}^{n}\left(\sum_{j=1}^{n} b_j p_{ij}\right)\mathbf{u}_i = \sum_{i=1}^{n} a_i\mathbf{u}_i$$

Tedy

$$a_i = \sum_{j=1}^{n} b_j p_{ij} \quad \forall j = 1, \ldots, n$$

Tedy $(a_1, \ldots, a_n)^T = \mathbf{P}(b_1, \ldots, b_n)^T$ □

Definice 11.4 *Jsou-li* $\mathcal{U} = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ *a* $\mathcal{V} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ *jsou dvě báze prostoru* $\mathbf{T}^n$ *a* $\mathbf{v}_j = \sum_{i=1}^{n} p_{ij}\mathbf{u}_i$, *pak matici* (p_{ij}) *nazýváme* matice přechodu od báze $\mathcal{V}$ *k bázi* $\mathcal{U}$.

Tvrzení 11.5 *Nechť* $\mathcal{U} = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$, $\mathcal{V} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ *a* $\mathcal{W} = \{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ *jsou tři báze prostoru* $\mathbf{T}^n$, $\mathbf{P}$ *je matice přechodu od báze* $\mathcal{V}$ *k bázi* $\mathcal{U}$ *a* $\mathbf{Q}$ *je matice přechodu od báze* $\mathcal{W}$ *k bázi* $\mathcal{V}$, *pak* $\mathbf{PQ}$ *je matice přechodu od báze* $\mathcal{W}$ *k bázi* $\mathcal{V}$.

Důkaz.

$$\mathbf{v}_j = \sum_{i=1}^{n} p_{ij}\mathbf{u}_i, \mathbf{w}_k = \sum_{j=1}^{n} q_{jk}\mathbf{v}_j$$

Z definice matice přechodu:

$$\mathbf{w}_k = \sum_{j=1}^{n} q_{jk}\mathbf{v}_j = \sum_{j=1}^{n} q_{jk}\sum_{i=1}^{n} p_{ij}\mathbf{u}_i = \sum_{i=1}^{n}\left(\sum_{j=1}^{n} p_{ij}q_{jk}\right)\mathbf{u}_i$$

Označíme $\mathbf{R} = (r_{ik})$ matici přechodu od $\mathcal{W}$ k $\mathcal{U}$. Pak

$$r_{ik} = \sum_{j=1}^{n} p_{ij}q_{jk} \quad \forall i, k$$

. Tedy $\mathbf{R} = \mathbf{PQ}$

□

Tvrzení 11.6 *Matice přechodu* $\mathbf{P}$ *od báze* $\mathcal{V}$ *k bázi* $\mathcal{U}$ *je regulární. Inverzní matice* $\mathbf{P}^{-1}$ *je matice přechodu od báze* $\mathcal{U}$ *k bázi* $\mathcal{V}$.

Důkaz. Použijeme Tvrzení 11.5 na případ $\mathcal{W} = \mathcal{U}$. Označíme $\mathbf{Q}$ matici přechodu od $\mathcal{U}$ k $\mathcal{V}$. Podle Tvrzení 11.5 je $\mathbf{PQ}$ matice přechodu od $\mathcal{U}$ k $\mathcal{U}$.
$\mathbf{u}_j = \mathbf{u}_j \quad \forall j$, tedy matice přechodu od $\mathcal{U}$ k $\mathcal{U}$ je $\mathbf{I}_n$.
$\mathbf{PQ} = \mathbf{I}_n \Rightarrow \mathbf{Q} = \mathbf{P}^{-1}$ (jsou čtvercové, tedy regulární).
□

Definice 11.5 *Matice lineárního zobrazení* $A : \mathbf{T}^n \to \mathbf{T}^m$ *vzhledem k bázi* $\mathcal{U} = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ *v* $\mathbf{T}^n$ *a bázi* $\mathcal{V} = \{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ *v* $\mathbf{T}^m$ *je* r_{ij}, *kde* $A(\mathbf{u}_j) = \sum_{i=1}^{m} r_{ij}\mathbf{v}_i$. *Matice lineárního zobrazení* $A : \mathbf{T}^n \to \mathbf{T}^n$ *vzhledem k bázi* $\mathcal{U} = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$.

Poznámka. Je-li $A : \mathbf{T}^n \to \mathbf{T}^m$ určené maticí $\mathbf{A}$, pak $\mathbf{A}$ je matice A vzhledem ke standardním bázím v obou prostorech.

Tvrzení 11.7 *Jsou-li* $A : \mathbf{T}^n \to \mathbf{T}^m$ *a* $B : \mathbf{T}^m \to \mathbf{T}^p$ *lineární zobrazení, je-li* $\mathcal{U} = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ *báze v* $\mathbf{T}^n$, $\mathcal{V} = \{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ *báze v* $\mathbf{T}^m$, $\mathcal{W} = \{\mathbf{w}_1, \ldots, \mathbf{w}_p\}$ *v* $\mathbf{T}^p$, $\mathbf{Q} = (q_{jk})$ *matice lineárního zobrazení* A *vzhledem k bázím* $\mathcal{U}$ *a* $\mathcal{V}$ *a* $\mathbf{P} = (p_{ij})$ *matice* B *vzhledem k bázím* $\mathcal{V}$ *a* $\mathcal{W}$, *pak součin* $\mathbf{PQ}$ *je matice lineárního zobrazení* $BA : \mathbf{T}^n \to \mathbf{T}^p$ *vzhledem k bázím* $\mathcal{U}$ *a* $\mathcal{W}$.

Důkaz.

$$A(\mathbf{u}_k) = \sum_{j=1}^{m} p_{jk}\mathbf{v}_j, \quad B(\mathbf{v}_j) = \sum_{i=1}^{p} q_{ij}\mathbf{w}_i$$

$$BA(\mathbf{u}_k) = B\left(\sum_{j=1}^{m} p_{jk}\mathbf{v}_j\right) = \sum_{j=1}^{m} p_{jk}B(\mathbf{v}_j) = \sum_{j=1}^{m} p_{jk}\left(\sum_{i=1}^{p} q_{ij}\mathbf{w}_i\right) =$$

$$= \sum_{j=1}^{m}\sum_{i=1}^{p} p_{jk}q_{ij}\mathbf{w}_i = \sum_{i=1}^{p}\left(\sum_{j=1}^{m} q_{ij}p_{jk}\right)\mathbf{w}_i = \ldots$$

Pozn.: $\sum_{j=1}^{m} q_{ij}p_{jk}$ je prvek na místě (i,k) v $\mathbf{QP}$;
označíme $\mathbf{QP} = (r_{ik})$

$$\ldots = \sum_{i=1}^{p} r_{ik}\mathbf{w}_i$$

□

Tvrzení 11.8 *Matice přechodu od $\mathcal{V}$ k $\mathcal{U}$ je matice identického zobrazení $I : \mathbf{T}^n \to \mathbf{T}^n$ vzhledem k bázím $\mathcal{V}$ a $\mathcal{U}$.*

Důkaz. Označíme $\mathbf{R} = (r_{ij})$ matici přechodu od $\mathcal{V}$ k $\mathcal{U}$, potom

$$I(\mathbf{v}_j) = \mathbf{v}_j = \sum_{i=1}^{n} r_{ij}\mathbf{u}_i$$

Tedy $\mathbf{R}$ je matice I vzhledem k bázím $\mathcal{V}$ a $\mathcal{U}$. □

Tvrzení 11.9 *Je-li $\mathbf{A}_\mathcal{U}$ matice $A : \mathbf{T}^n \to \mathbf{T}^n$ vzhledem k bázi $\mathcal{U} = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$, $\mathbf{A}_\mathcal{V}$ matice A vzhledem k bázi $\mathcal{V} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ a $\mathbf{P}$ matice přechodu od báze $\mathcal{V}$ k bázi $\mathcal{U}$, pak $\mathbf{A}_\mathcal{V} = \mathbf{P}^{-1}\mathbf{A}_\mathcal{U}\mathbf{P}$.*

Důkaz.
(pomocný obrázek:)

$$\begin{array}{ccccccc} \mathbf{T}^n & \overset{I}{\leftarrow} & \mathbf{T}^n & \overset{A}{\leftarrow} & \mathbf{T}^n & \overset{I}{\leftarrow} & \mathbf{T}^n \\ \mathcal{V} & \mathbf{P}^{-1} & \mathcal{U} & \mathbf{A}_\mathcal{U} & \mathcal{U} & \mathbf{P} & \mathcal{V} \end{array}$$

$\mathbf{P}$ je matice přechodu od $\mathcal{V}$ k $\mathcal{U}$.
$\mathbf{A}_\mathcal{U}$ je matice lieárního zobrazení A vzhledem k bázi $\mathcal{U}$.
$\mathbf{P}^{-1}$ je matice přechodu od $\mathcal{U}$ k $\mathcal{V}$.
$\mathbf{A}_\mathcal{V} = \mathbf{P}^{-1}\mathbf{A}_\mathcal{U}\mathbf{P}$ □