Matematický ústav Slezské univerzity v Opavě
Učební texty k přednášce ALGEBRA I, zimní semestr 2000/2001
Michal Marvan

# 6. Matice. Algebraické vlastnosti

## 1. Algebraické operace s maticemi

**Definice.** Buďte $A$, $B$ matice jednoho a téhož typu $r/s$ nad polem $P$. Jejich *součet* je matice $A+B$ téhož typu $r/s$, daná předpisem

$$(A+B)_{ij} = A_{ij} + B_{ij}$$

pro každé $i = 1, \ldots, r$ a $j = 1, \ldots, s$.

Dále definujeme *c-násobek* matice $A$, kde $c$ je libovolný prvek pole $P$, jako matici $cA$ typu $r/s$ danou předpisem

$$(cA)_{ij} = cA_{ij}$$

pro každé $i = 1, \ldots, r$ a $j = 1, \ldots, s$.

**Příklad.** Nechť

$$A = \begin{pmatrix} 1 & -3 & 2 \\ 2 & 4 & -1 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 11 & 2 \\ 2 & -5 & -1 \end{pmatrix}.$$

Pak

$$A+B = \begin{pmatrix} 1 & 8 & 4 \\ 4 & -1 & -2 \end{pmatrix}, \qquad 2B = \begin{pmatrix} 0 & 22 & 4 \\ 4 & -10 & -2 \end{pmatrix}.$$

**Definice.** *Nulová* matice je matice 0 složená ze samých nul. Matice $(-1)A$ se značí $-A$ a nazývá se matice *opačná* k matici $A$.

**Tvrzení.** *Nechť jsou $A$, $B$, $C$ matice nad polem $P$. Pak platí*

(1) $A+B = B+A$,
(2) $A+(B+C) = (A+B)+C$,
(3) $A+0 = A$,
(4) $A+(-A) = 0$,
(5) $1A = A$,
(6) $c(A+B) = cA+cB$,
(7) $(c+k)A = cA+kA$,
(8) $c(kA) = (ck)A$,

*pokud jsou všechny naznačené operace definovány.*

**Důkaz.** (1) $(A+B)_{ij} = A_{ij} + B_{ij} = B_{ij} + A_{ij} = (B+A)_{ij}$. (2)–(8) Cvičení.

Množinu všech matic typu $r/s$ nad polem $P$ označme $M_{rs}(P)$. Podle (1)–(4) z předchozího tvrzení, $M_{rs}(P)$ je abelovská grupa. [Jak uvidíme později, axiomy (1)–(8) říkají, že $M_{rs}(P)$ je vektorový prostor nad polem $P$.]

Zavádíme i součin $A \cdot B$ dvou matic, má-li matice $A$ právě tolik sloupců, kolik má $B$ řádků. Výsledkem je matice $C = A \cdot B$, která má stejný počet řádků jako matice $A$ a stejný počet sloupců jako matice $B$. Prvek $C_{kl}$ na průsečíku $k$-tého řádku a $l$-tého sloupce dostaneme tak, že po řadě násobíme mezi sebou prvky $k$-tého řádku matice $A$ a prvky $l$-tého sloupce matice $B$ a vzniklé součiny (v počtu $s$) sečteme:

**Definice.** Buď $A$ matice typu $r/s$, buď $B$ matice typu $s/t$ nad polem $P$, Jejich *součin* je matice $A \cdot B$ typu $r/t$ daná předpisem

$$\begin{aligned}(A \cdot B)_{kl} &= A_{k1}B_{1l} + A_{k2}B_{2l} + \cdots + A_{ks}B_{sl} \\ &= \sum_{i=1}^{s} A_{ki}B_{il}.\end{aligned}$$

Znaménko „$\cdot$“ často vynecháváme a píšeme jednoduše $AB$.

Součin matic představuje zobrazení $M_{rs} \times M_{st} \to M_{rt}$.

**Příklad.** Nechť

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

Pak

$$C = AB = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix},$$

protože $C_{11} = A_{11}B_{11} + A_{12}B_{21} = 1 \cdot 0 + 1 \cdot 0 = 0$, podobně $C_{12} = A_{11}B_{12} + A_{12}B_{22} = 1 \cdot 1 + 1 \cdot 1 = 2$, atd. V obráceném pořadí

$$BA = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Může se tedy stát, že oba součiny $AB$ a $BA$ existují, a přesto si nejsou rovny. Tudíž, násobení matic obecně není komutativní. Dále je vidět, že součin nenulových matic může být nulová matice.

**Definice.** *Čtvercová* matice je matice typu $n/n$, tj. matice, která má stejný počet řádků jako sloupců.

Součin takových matic je zase čtvercová matice typu $n/n$. Tudíž, násobení čtvercových matic je binární operace.

**Definice.** *Jednotková* matice je čtvercová matice tvaru

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

To jest,

$$E_{ij} = \begin{cases} 1 & \text{když } i = j, \\ 0 & \text{když } i \neq j. \end{cases}$$

**Tvrzení.** *Nechť jsou $A$, $B$, $C$ matice nad polem $P$. Pak platí*

$$(9) \quad A(BC) = (AB)C,$$
$$(10) \quad AE = EA = A,$$
$$(11) \quad A(B + C) = AB + AC,$$
$$(12) \quad (A + B)C = AC + BC,$$

*pokud jsou všechny naznačené operace definovány.*

Podle (9) a (10) je $M_{nn}(P)$ monoid vzhledem k operaci násobení matic. Neutrálním prvkem je jednotková matice.

**Důkaz.** Dokažme například identitu (11) za předpokladu, že $A$ je matice typu $r/s$ a $B$, $C$ jsou matice typu $s/t$. Matici na levé straně označme $U$, matici na pravé straně označme $V$. Pak $U$ i $V$ jsou shodně typu $r/t$ a platí

$$U_{kl} = \sum_{i=1}^{s} A_{ki}(B + C)_{il} = \sum_{i=1}^{s} A_{ki}(B_{il} + C_{il}) = \sum_{i=1}^{s} (A_{ki}B_{il} + A_{ki}C_{il})$$
$$= \sum_{i=1}^{s} A_{ki}B_{il} + \sum_{i=1}^{s} A_{ki}C_{il} = (AB)_{kl} + (AC)_{kl} = V_{kl}.$$

Ostatní identity se dokazují analogicky. Jde o dobré cvičení.

## 2. Inverzní matice

Budeme řešit problém rozpoznání invertibilních prvků v monoidu $M_{nn}(P)$.

**Definice.** Buď $A$ čtvercová matice typu $n/n$. Řekneme, že matice $X$ je *inverzní* k matici $A$, je-li téhož typu $n/n$ a platí

$$AX = XA = E.$$

Značí se $X = A^{-1}$. Matice $A$ se nazývá *invertibilní*, existuje-li matice k ní inverzní.

K dané čtvercové matici $A$ existuje nejvýše jedna inverzní matice [v libovolném monoidu existuje k danému prvku nejvýše jeden prvek inverzní].

Příklad: každá jednotková matice je invertibilní a platí $E^{-1} = E$. Neinvertibilní je například nulová matice (dokažte).

Invertibilní nejsou ani matice $A$, $B$ z posledního příkladu: Kdyby matice $A$ měla inverzní matici $A^{-1}$, pak bychom měli $B = BE = B(AA^{-1}) = (BA)A^{-1} = 0A^{-1} = 0$, spor. Podobně pro $B$.

**Tvrzení.** *Nechť jsou $A$, $B$ invertibilní matice.*
(1) *Pak je invertibilní i matice $AB$ a platí $(AB)^{-1} = B^{-1}A^{-1}$;*
(2) *Invertibilní je i matice $A^{-1}$ a platí $(A^{-1})^{-1} = A$.*

**Důkaz.** Tvrzení platí v libovolném monoidu a byla již dokázána.

**Důsledek.** *Invertibilní matice tvoří podgrupu v monoidu $M_{nn}(P)$.*

**Definice.** Grupa invertibilních čtvercových matic se značí $\mathrm{GL}_n(P)$. Nazývá se *obecná lineární grupa*.

Potřebujeme praktická kriteria pro invertibilitu matic. Jedno z nich je nalezeno níže, přitom také dostáváme algoritmus, který invertuje zadanou matici, pokud je invertibilní. Klíčem k úspěchu je Gaussův–Jordanův tvar a tzv. elementární matice.

**Definice.** *Elementární matice* jsou čtvercové matice jednoho z následujících tvarů:

(i) $$E_{ij}(c) = \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ & \cdots & & \cdots & & \cdots & \\ 0 & \cdots & 1 & \cdots & c & \cdots & 0 \\ & \cdots & & \cdots & & \cdots & \\ 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ & \cdots & & \cdots & & \cdots & \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \begin{matrix} \\ \\ i \\ \\ j \\ \\ \\ \end{matrix}$$

kde $i \neq j$, $c \neq 0$. Matice $E_{ij}(c)$ se od jednotkové matice liší tím, že prvek $E_{ij}$ je roven $c$.

(ii) $$E_i(c) = \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 \\ & \cdots & & \cdots & \\ 0 & \cdots & c & \cdots & 0 \\ & \cdots & & \cdots & \\ 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \begin{matrix} \\ \\ i \\ \\ \\ \end{matrix}$$

kde $c \neq 0$. Matice $E_i(c)$ se od jednotkové matice liší tím, že prvek $E_{ii}$ je roven $c$.

(iii) $$E_{ij} = \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ & \cdots & & \cdots & & \cdots & \\ 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ & \cdots & & \cdots & & \cdots & \\ 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 \\ & \cdots & & \cdots & & \cdots & \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \begin{matrix} \\ \\ i \\ \\ j \\ \\ \\ \end{matrix}$$

kde $i \neq j$. Matice $E_{ij}$ se od jednotkové matice liší tím, že $i$-tý a $j$-tý řádek jsou vyměněny.

Všimněte si, že každá z elementárních matic $E_{ij}(c)$, $E_i(c)$, $E_{ij}$ vznikne z jednotkové matice $E$ aplikací jedné ze tří elementárních řádkových úprav, popsaných v minulé přednášce.

**Lemma.** *Buďte $A$, $A'$ dvě matice téhož typu. Následující výroky jsou ekvivalentní:*
1° *matice $A'$ vznikne z $A$ jednou z elementárních řádkových úprav;*
2° *existuje elementární matice $Q$ taková, že $A' = QA$.*

**Důkaz.** Elementární matice odpovídají po řadě elementárním úpravám (i) přičtení k $i$-tému řádku $c$-násobku $j$-tého řádku; (ii) vynásobení $i$-tého řádku prvkem $c \in P \setminus \{0\}$; (iii) výměna $i$-tého a $j$-tého řádku. Důkaz se ve všech třech případech snadno provede přímým výpočtem.

**Lemma.** *Elementární matice jsou vesměs invertibilní a platí*
(i) $(E_i(c))^{-1} = E_i(c^{-1})$,
(ii) $(E_{ij}(c))^{-1} = E_{ij}(-c)$,
(iii) $(E_{ij})^{-1} = E_{ij}$.

**Důkaz.** Cvičení. Opět se vše snadno ověří přímým výpočtem.

Nyní zformulujeme důležité kriterium invertibility

**Tvrzení.** *Čtvercová matice $A$ je invertibilní právě tehdy, když je řádkově ekvivalentní s jednotkovou maticí.*

**Důkaz.** „⇒“: Buď $A$ matice, řádkově ekvivalentní s jednotkovou maticí $E$. Pak existuje konečná posloupnost řádkových úprav, která převede $A$ na $E$. Označme $Q_1, Q_2, \ldots, Q_k$ elementární matice, odpovídající jednotlivým úpravám. Pak $Q_k \cdots Q_2 Q_1 A = E$ (v tomto pořadí!). Označme $Q = Q_k \cdots Q_2 Q_1$, máme pak

$$QA = E.$$

Ovšem každá z matic $Q_1, Q_2, \ldots, Q_k$ je invertibilní, a proto je invertibilní i jejich součin (a platí $Q^{-1} = Q_1^{-1} Q_2^{-1} \cdots Q_k^{-1}$). Rovnost $QA = E$ proto můžeme na obou stranách vynásobit zleva maticí $Q^{-1}$. Dostáváme $A = Q^{-1}QA = Q^{-1}E = Q^{-1}$. Tudíž, $A^{-1} = (Q^{-1})^{-1} = Q$ a $A$ je invertibilní.

„⇐“: Nechť je, naopak, $A$ invertibilní čtvercová matice typu $n/n$. Převeďme $A$ řádkovými úpravami na Gaussův–Jordanův tvar $B$, takže $A \sim B$. Rozeznávejme dva případy.

1. Nechť během algoritmu nalezneme právě $n$ hlavních prvků; ty pak nutně vyplňují úhlopříčku, jsou rovny 1 a nad nimi i pod nimi leží nuly. To ovšem znamená, že $B = E$, takže $A \sim E$, což se mělo dokázat.

2. Nechť bylo nalezeno méně než $n$ hlavních prvků, pak $B$ je matice s nulovým posledním řádkem (proč?), načež pro každou matici $X$ typu $n/n$ je součin $BX$ zase matice s nulovým posledním řádkem (ověřte).

Nicméně, $B = QA$, kde $Q$ je součin elementárních matic, a tedy $B$ je též invertibilní (je součinem invertibilních matic), tj. existuje $B^{-1}$. Volba $X = B^{-1}$ pak vede ke sporu, protože $BB^{-1} = E$, ale $E$ nemá nulový poslední řádek.

Navrhněme postup, jak matici $A^{-1}$ spočítat. Podle důkazu předchozího tvrzení $A^{-1} = Q = Q_k \cdots Q_2 Q_1 = Q_k \cdots Q_2 Q_1 E$, což je matice, která vznikne z jednotkové matice $E$ posloupností elementárních řádkových úprav, příslušných elementárním maticím $Q_1, Q_2, \ldots, Q_k$. Tedy toutéž posloupností, která převedla $A$ na $E$:

$$A \to E$$
$$E \to A^{-1}.$$

Stačí tedy, aby se řádkové úpravy, prováděné s maticí $A$ při převodu na $E$, prováděly současně i s maticí $E$, a ta pak přejde v $Q = A^{-1}$:

**Algoritmus** (výpočet inverzní matice). Buď $A$ čtvercová matice typu $n/n$. Připojme k $A$ z pravé strany jednotkovou matici $E$:

$$\left(\begin{array}{cccc|cccc} A_{11} & A_{12} & \cdots & A_{1s} & 1 & 0 & \cdots & 0 \\ A_{21} & A_{22} & \cdots & A_{2s} & 0 & 1 & \cdots & 0 \\ & & \cdots & & & & \cdots & \\ A_{r1} & A_{r2} & \cdots & A_{rs} & 0 & 0 & \cdots & 1 \end{array}\right),$$

a v takto vzniklé matici typu $n/2n$ provádějme řádkové úpravy, které levou část (tj. matici $A$) převedou na Gaussův–Jordanův tvar $B$. Potom:

– jestliže $B = E$, pak $A$ je invertibilní a na pravé straně vyjde inverzní matice $A^{-1}$;

– jestliže $B$ obsahuje nulový řádek, pak $A$ není invertibilní.

**Příklad.** Výpočet inverzní matice:

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

**Příklad.** Neinvertibilní případ:

$$\left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 3 & 6 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & 0 & -3 & 1 \end{array}\right).$$

**Cvičení.** Invertujte matice

$$\begin{pmatrix} \mathrm{i} & 1 \\ 2\mathrm{i} & \mathrm{i}+1 \end{pmatrix},$$

resp.

$$\begin{pmatrix} [2]_5 & [1]_5 \\ [3]_5 & [2]_5 \end{pmatrix}.$$

**Cvičení.** Písmena ABCDEFGHIJKLMNOPQRSTUVWXYZ nechť mají po řadě kódy $[1]_{31}$ až $[26]_{31}$. Kód $[0]_{31}$ nechť označuje mezeru. Kódy $[27]_{31}$ až $[30]_{31}$ přiřaďme znakům „čárka“, „tečka“, „vykřičník“ a „otazník“. Například zprávě „HIC SUNT LEONES!“ odpovídá posloupnost $[8]_{31}$ $[9]_{31}$ $[3]_{31}$ $[0]_{31}$ $[19]_{31}$ $[21]_{31}$ $[14]_{31}$ $[20]_{31}$ $[0]_{31}$ $[12]_{31}$ $[5]_{31}$ $[15]_{31}$ $[14]_{31}$ $[5]_{31}$ $[19]_{31}$ $[29]_{31}$. Již Jules Verne seznámil světovou mládež se způsobem, jak podobné zprávy dekódovat, jsou-li dostatečně dlouhé a známe-li průměrnou četnost výskytu jednotlivých písmen v jazyce zprávy. Dekódování se ztíží, kódujeme-li $n$-tice znaků. Nechť pro jednoduchost $n = 2$. Posloupnost rozdělme na dvojice prvků ze $\mathbf{Z}_{31}$ (počínaje zleva) a každou dvojici, považovanou za matici typu $2/1$, vynásobme zleva maticí

$$A = \begin{pmatrix} [12]_{31} & [10]_{31} \\ [13]_{31} & [11]_{31} \end{pmatrix}.$$

Vznikne posloupnost $[0]_{31}$ $[17]_{31}$ $[5]_{31}$ $[8]_{31}$ $[4]_{31}$ $[13]_{31}$ $[27]_{31}$ $[30]_{31}$ $[27]_{31}$ $[8]_{31}$ $[24]_{31}$ $[13]_{31}$ $[1]_{31}$ $[20]_{31}$ $[22]_{31}$ $[8]_{31}$, které odpovídá posloupnost znaků k odeslání: „ QEHDM,?,HXMATVH“. Původní text pak zjistíme použitím inverzní matice

$$A^{-1} = \begin{pmatrix} [21]_{31} & [26]_{31} \\ [9]_{31} & [6]_{31} \end{pmatrix}$$

analogickým způsobem (cvičení).

**Problém k řešení.** Dekódujte

„KRRWZ WRNC.LENANADFOWOTU?BZPKA WC EUZPCQ,?YDP?!AQXBB“

## 3. Transponovaná matice

**Definice.** *Transponovaná matice* k matici $A \in M_{rs}(P)$ je matice $A^\top \in M_{sr}(P)$, splňující

$$A^\top_{ij} = A_{ji}.$$

**Příklad.**

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^\top = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$$

Všimněte si, že řádky se zaměnily za sloupce a naopak.

Předpisem $A \mapsto A^\top$ je zadáno zobrazení $(\cdot)^\top : M_{rs}(P) \to M_{sr}(P)$.

**Cvičení.** Ukažte, že $(\cdot)^\top : M_{rs}(P) \to M_{sr}(P)$ je homomorfismus aditivních grup.

**Cvičení.** $(AB)^\top = B^\top A^\top$ pro libovolné matice $A \in M_{rs}(P)$ a $B \in M_{st}(P)$. Dokažte.

**Cvičení.** Nechť $A \in \mathrm{GL}_n(P)$. Dokažte, že $A^\top \in \mathrm{GL}_n(P)$ a že platí

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

Víme již, že elementární řádková úprava je totéž, co násobení elementární maticí zleva. Elementární sloupcová úprava se zavádí analogicky jako řádková, pouze slovo řádek se v definici všude nahradí slovem sloupec. Protože transponování matic vede k vzájemné záměně řádků za sloupce, libovolná elementární sloupcová úprava matice $A$ se získá kombinací

$$\text{transpozice} \to \text{elementární řádková úprava} \to \text{transpozice}.$$

Je-li $Q$ matice příslušná elementární řádkové úpravě, pak právě naznačeným postupem převedeme matici $A$ na matici $A \mapsto A^\top \mapsto QA^\top \mapsto (QA^\top)^\top = (A^\top)^\top Q^\top = AQ^\top$. Vidíme, že elementární sloupcová úprava je totéž, co násobení maticí $Q^\top$ zprava. Přitom matice transponovaná k elementární matici je opět elementární matice:

$$E_i(c)^\top = E_i(c), \qquad E_{ij}(c)^\top = E_{ji}(c), \qquad E_{ij}^\top = E_{ji} = E_{ij}.$$

O sloupcových úpravách matic platí analogická tvrzení jako o řádkových úpravách. Pozor je třeba dávat při řešení soustav lineárních rovnic. Sloupcové úpravy matice soustavy *mění* řešení rovnice. (Například záměna sloupců = záměna neznámých.)

Také ve výše uvedeném algoritmu pro výpočet inverzní matice *nelze* provádět sloupcové úpravy současně s řádkovými, ani za předpokladu, že je provedeme v obou polovinách matice $n/2n$. To lze ověřit na prakticky libovolném příkladě výpočtu inverzní matice.