Matice

Nechť $(R, +, \cdot)$ je okruh a nechť m, n jsou přirozená čísla. Matice typu m/n nad okruhem $(R, +, \cdot)$ vznikne, když libovolných $m{\cdot}n$ prvků z R naskládáme do obdélníkového schematu o m řádcích a n sloupcích. Formálně se **matice typu** m/n nad okruhem $(R, +, \cdot)$ definuje jako libovolné zobrazení

$$A : \{1, 2, \ldots, m\} \times \{1, 2, \ldots, n\} \to R\,.$$

Označíme-li pro každá $i \in \{1, 2, \ldots, m\}$, $j \in \{1, 2, \ldots, n\}$ pomocí a_{ij} hodnotu v R, kterou zobrazení A přiřazuje dvojici (i, j), pak obvyklý způsob, jak se matice A zapisuje, je ve tvaru

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}.$$

Pak prvek a_{ij} leží v i-tém řádku a v j-tém sloupci matice A. Stručněji se tato matice často zapisuje ve tvaru

$$A = (a_{ij})_{i=1,\ldots,m,\, j=1,\ldots,n}$$

anebo jen ve tvaru $A = (a_{ij})$ s udáním, že jde o matici typu m/n.

Matici typu m/n, jejíž všechny prvky jsou rovny nulovému prvku 0 okruhu $(R, +, \cdot)$, značíme jako O_{mn} anebo stručně jen jako O a říkáme, že je to **nulová matice**.

Přistoupíme k definicím operací s maticemi. Pro libovolné dvě matice $A = (a_{ij})$ a $B = (b_{ij})$ téhož typu m/n nad okruhem $(R, +, \cdot)$ definujeme jejich **součet** $A + B$ jako matici $C = (c_{ij})$ typu m/n, kde pro každá $i \in \{1, 2, \ldots, m\}$ a $j \in \{1, 2, \ldots, n\}$ je $c_{ij} = a_{ij} + b_{ij}$. Takže lze psát, že $A + B = (a_{ij} + b_{ij})$.

Dále pro libovolnou matici $A = (a_{ij})$ typu m/n nad okruhem $(R, +, \cdot)$ a pro libovolný prvek $c \in R$ definujeme **násobek** $c{\cdot}A$

matice A prvkem c jako matici $D = (d_{ij})$ typu m/n, kde pro každá $i \in \{1, 2, \dots, m\}$ a $j \in \{1, 2, \dots, n\}$ je $d_{ij} = c{\cdot}a_{ij}$. Takže lze psát, že $c{\cdot}A = (c{\cdot}a_{ij})$.

Zejména můžeme k dané matici $A = (a_{ij})$ uvažovat matici $(-1){\cdot}A$, kterou značíme jako $-A$. (Zde 1 je jednotkový prvek okruhu $(R, +, \cdot)$ a -1 je prvek k němu opačný.) Víme totiž, že pro libovolný prvek $a \in R$ platí $(-1){\cdot}a = -(1{\cdot}a) = -a$. To znamená, že pak máme $-A = (-a_{ij})$. O matici $-A$ říkáme, že je to matice **opačná** k matici A. Je jasné, že pak platí $A + (-A) = O$.

Označíme-li symbolem $\mathrm{Mat}_{mn}(R)$ množinu všech matic typu m/n nad okruhem $(R, +, \cdot)$, pak sčítání matic je binární operací na množině $\mathrm{Mat}_{mn}(R)$ a je zřejmý následující fakt.

Tvrzení. $(\mathrm{Mat}_{mn}(R), +)$ je komutativní grupa.

Pro libovolnou matici $A = (a_{ij})$ typu m/n a libovolnou matici $B = (b_{jk})$ typu n/p, obě nad okruhem $(R, +, \cdot)$, definujeme jejich **součin** $A \cdot B$ jako matici $C = (c_{ik})$ typu m/p, kde pro každá $i \in \{1, 2, \dots, m\}$ a $k \in \{1, 2, \dots, p\}$ klademe

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

Takto definované násobení matic je asociativní:

Tvrzení. Pro libovolnou matici $A = (a_{ij})$ typu m/n, pro libovolnou matici $B = (b_{jk})$ typu n/p a pro libovolnou matici $C = (c_{k\ell})$ typu p/q, všechny nad okruhem $(R, +, \cdot)$, platí

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C.$$

Důkaz. Podle definice součinu matic máme $A \cdot B = D$, kde $D = (d_{ik})$ je matice typu m/p, přičemž pro libovolná i, k máme $d_{ik} = \sum_{j=1}^{n} a_{ij} \cdot b_{jk}$. Dále máme $(A \cdot B) \cdot C = D \cdot C = F$, kde

$F = (f_{i\ell})$ je matice typu m/q, přičemž pro libovolná i, ℓ máme

$$f_{i\ell} = \sum_{k=1}^{p} d_{ik} \cdot c_{k\ell} = \sum_{k=1}^{p} \Big(\sum_{j=1}^{n} a_{ij} \cdot b_{jk} \Big) \cdot c_{k\ell}.$$

Podobně máme $B \cdot C = G$, kde $G = (g_{j\ell})$ je matice typu n/q, přičemž pro libovolná j, ℓ máme $g_{j\ell} = \sum_{k=1}^{p} b_{jk} \cdot c_{k\ell}$. Dále máme $A \cdot (B \cdot C) = A \cdot G = H$, kde $H = (h_{i\ell})$ je matice typu m/q, přičemž pro libovolná i, ℓ máme

$$h_{i\ell} = \sum_{j=1}^{n} a_{ij} \cdot g_{j\ell} = \sum_{j=1}^{n} a_{ij} \cdot \Big(\sum_{k=1}^{p} b_{jk} \cdot c_{k\ell} \Big).$$

Odtud ovšem s využitím distributivity a asociativity násobení v okruhu $(R, +, \cdot)$ pro libovolná i, ℓ dostáváme

$$h_{i\ell} = \sum_{j=1}^{n} \sum_{k=1}^{p} a_{ij} \cdot b_{jk} \cdot c_{k\ell} = \sum_{k=1}^{p} \sum_{j=1}^{n} a_{ij} \cdot b_{jk} \cdot c_{k\ell} = f_{i\ell}.$$

To znamená, že $H = F$, což bylo třeba ukázat.

Násobení matic je dále distributivní vůči sčítání matic:

Tvrzení. Pro libovolnou matici $A = (a_{ij})$ typu m/n a pro libovolné matice $B = (b_{jk})$ a $C = (c_{jk})$, obě typu n/p, přitom vše nad okruhem $(R, +, \cdot)$, platí

$$A \cdot (B + C) = A{\cdot}B + A{\cdot}C.$$

Pro libovolné matice $F = (f_{ij})$ a $G = (g_{ij})$, obě typu m/n, a pro libovolnou matici $H = (h_{jk})$ typu n/p, přitom všechny matice nad okruhem $(R, +, \cdot)$, platí

$$(F + G) \cdot H = F{\cdot}H + G{\cdot}H.$$

Důkaz obou rovností se provede podobným způsobem jako důkaz předchozího tvrzení přímým použitím definic sčítání a násobení matic s využitím distributivity v okruhu $(R, +, \cdot)$.

Matice nad okruhem $(R, +, \cdot)$ mající týž počet řádků jako sloupců, to znamená matice typu n/n pro nějaké přirozené číslo n se nazývají **čtvercové matice řádu** n. Je-li $A = (a_{ij})$ taková čtvercová matice řádu n, pak o prvcích a_{ii} pro $i = 1, 2, \ldots, n$ říkáme, že tvoří **hlavní diagonálu** matice A.

Čtvercovou matici řádu n nad netriviálním okruhem $(R, +, \cdot)$, v níž všechny prvky na hlavní diagonále jsou rovny jednotkovému prvku 1 zmíněného okruhu a všechny ostatní prvky jsou rovny nulovému prvku 0 tohoto okruhu, označujeme symbolem E_n nebo krátce jen E. Máme tedy

$$E_n = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix},$$

kde je celkem n řádků a n sloupců. O matici E_n říkáme, že je to **jednotková matice** řádu n. Bezprostředně z definice násobení matic totiž plyne, že pro libovolnou matici $A = (a_{ij})$ typu m/n nad zmíněným okruhem $(R, +, \cdot)$ platí $E_m \cdot A = A = A \cdot E_n$.

V souladu s označením zavedeným výše symbolem $\mathrm{Mat}_{nn}(R)$ značíme množinu všech čtvercových matic řádu n nad okruhem $(R, +, \cdot)$. Pak vedle sčítání také násobení matic je binární operací na množině $\mathrm{Mat}_{nn}(R)$ a je evidentní následující fakt.

Tvrzení. $(\mathrm{Mat}_{nn}(R), +, \cdot)$ je okruh.

Poznamenejme, že je-li okruh $(R, +, \cdot)$ netriviální, pak byť by třeba byl sám komutativní, pro $n > 1$ okruh $(\mathrm{Mat}_{nn}(R), +, \cdot)$ není komutativní a navíc obsahuje dělitele nuly:

Vezměme například matici $C_n = (c_{ij})$ řádu n, kde $c_{11} = 1$ a $c_{ij} = 0$ pro všechny ostatní dvojice indexů i, j, a dále matici $D_n = (d_{ij})$ řádu n, kde $d_{12} = 1$ a $d_{ij} = 0$ pro všechny ostatní dvojice indexů i, j. Pak $C_n \cdot D_n = D_n$, zatímco $D_n \cdot C_n = O_{nn}$.

Mějme matici

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

typu m/n nad okruhem $(R, +, \cdot)$. Uvažme matici $A^\top$ typu n/m, která vznikne z matice A záměnou řádků a sloupců, tedy matici

$$A^\top = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{12} & a_{22} & \dots & a_{m2} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \dots & a_{mn} \end{pmatrix}.$$

O matici $A^\top$ říkáme, že je to matice **transponovaná** k matici A.

Přímo z definice násobení matic pak plyne následující fakt:

Tvrzení. Je-li $(R, +, \cdot)$ komutativní okruh, pak pro libovolnou matici $A = (a_{ij})_{i=1,\dots,m,\, j=1,\dots,n}$ a pro libovolnou matici $B = (b_{jk})_{j=1,\dots,n,\, k=1,\dots,p}$, obě nad okruhem $(R, +, \cdot)$, platí

$$(A \cdot B)^\top = B^\top \cdot A^\top.$$

Důkaz. Nechť $A \cdot B = F$. Pak $F = (f_{ik})_{i=1,\dots,m,\, k=1,\dots,p}$, kde pro libovolná i, k je $f_{ik} = \sum_{j=1}^{n} a_{ij} \cdot b_{jk}$. Přitom $(A \cdot B)^\top = F^\top$, kde $F^\top = (f_{ik})_{k=1,\dots,p,\, i=1,\dots,m}$. Nechť dále $B^\top \cdot A^\top = G$. Pak poněvadž $A^\top = (a_{ij})_{j=1,\dots,n,\, i=1,\dots,m}$ a $B^\top = (b_{jk})_{k=1,\dots,p,\, j=1,\dots,n}$, máme $G = (g_{ki})_{k=1,\dots,p,\, i=1,\dots,m}$, kde $g_{ki} = \sum_{j=1}^{n} b_{jk} \cdot a_{ij}$ pro libovolné indexy k, i. Vzhledem ke komutativitě násobení v okruhu $(R, +, \cdot)$ odtud vychází, že $f_{ik} = g_{ki}$ pro všechny dvojice indexů k, i, takže $F^\top = G$. To bylo třeba dokázat.