I. ALGEBRAICKÝ ÚVOD

1. MNOŽINY A ZOBRAZENÍ

V tomto paragrafu připomeneme některé základní matematické pojmy a jejich vlastnosti, zavedeme několik symbolů a termínů; navíc stručně uvedeme některá důležitá fakta o množinách.

V celém textu budeme užívat následující označení:

$\mathbb{P}$ — množina všech prvočísel,
$\mathbb{N}$ — množina všech přirozených čísel, tj. $\mathbb{N} = \{1, 2, 3, \dots\}$,
$\mathbb{Z}$ — množina všech celých čísel,
$\mathbb{Q}$ — množina všech racionálních čísel,
$\mathbb{R}$ — množina všech reálných čísel,
$\mathbb{C}$ — množina všech komplexních čísel.

Budeme užívat i tzv. *kvantifikátory*; můžeme je chápat jako symboly pro následující slovní označení:

$$\forall \ \text{—} \ \text{pro každé} , \qquad \exists \ \text{—} \ \text{existuje} .$$

V celém textu budeme předpokládat znalost základních poznatků o množinách a množinových operacích (*podmnožina*, *sjednocení*, *průnik*, *rozdíl*, *kartézský součin* apod.).

Zdůrazněme, že nelze uvažovat *množinu všech množin* — to vede k logickým sporům; proto se na několika místech objeví termín *třída všech množin*.

Poznamenejme, že od množiny je třeba odlišovat *soubor*; zatímco množina obsahuje prvky navzájem různé, v souboru se mohou prvky i vícekrát opakovat. Např. $\{1, 1, 2, 1, 3, 2, 2, 3, 2, 3\}$ je soubor, který obsahuje prvek 1 třikrát, prvek 2 čtyřikrát a prvek 3 třikrát.

Často se setkáme s tzv. indexovaným souborem. Jsou-li Λ a X množiny, pak

$$\{x_\alpha \ ; \ \ \alpha \in \Lambda\} , \qquad \text{resp.} \qquad \{x_\alpha\}_{\alpha\in\Lambda}$$

je *indexovaný soubor* prvků množiny X, jestliže $x_\alpha \in X$ pro každé $\alpha \in \Lambda$ (indexy probíhají množinu Λ); znamená to, že každému $\alpha \in \Lambda$ je jednoznačně přiřazen prvek $x_\alpha \in X$. Znovu zdůrazněme, že jednotlivé prvky x_α nemusí být navzájem různé.

V následujícím odstavci budeme definovat zobrazení a některé jeho speciální typy; tyto pojmy je třeba dobře pochopit, závisí na tom porozumění celého dalšího textu.

1.1. Definice. *Zobrazením* f množiny A do množiny B rozumíme předpis, který každému prvku $a \in A$ přiřazuje právě jeden prvek $f(a) \in B$.

Zobrazení f se nazývá *prosté*, resp. *injektivní* (též *injekce*), jestliže různé prvky množiny A zobrazuje na různé prvky množiny B, tj.

$$\forall a_1, a_2 \in A \qquad a_1 \neq a_2 \implies f(a_1) \neq f(a_2) \ .$$

Řekneme, že zobrazení f je zobrazením množiny A *na* množinu B, resp. *surjektivním* zobrazením (též *surjekce*), jestliže na každý prvek množiny B se zobrazí alespoň jeden prvek množiny A, tj.

$$\forall b \in B \quad \exists a \in A \qquad f(a) = b \ .$$

Zobrazení, které je současně injektivní a surjektivní (tj. prosté a na), se nazývá *vzájemně jednoznačné*, resp. *bijektivní* (též *bijekce*). Bijektivní zobrazení f množiny A na množinu B je tedy charakterizováno touto podmínkou: pro každé $b \in B$ existuje právě jediný prvek $a \in A$, pro který je $f(a) = b$.

1.2. Příklady.

(i) Zobrazení, které každému číslu $n \in \mathbb{Z}$ přiřazuje číslo $-n$, je bijekce množiny $\mathbb{Z}$ na množinu $\mathbb{Z}$.

(ii) Zobrazení, které každému číslu $n \in \mathbb{Z}$ přiřazuje číslo $2n$, je injekce množiny $\mathbb{Z}$ do množiny $\mathbb{Z}$. Toto zobrazení není surjekce, a tedy ani bijekce.

(iii) Zobrazení, které každému číslu $n \in \mathbb{Z}$ přiřazuje číslo $|n|+1$, je surjekce množiny $\mathbb{Z}$ na množinu $\mathbb{N}$. Toto zobrazení není injekce, a tedy ani bijekce.

(iv) Zobrazení, které každému číslu $x \in \mathbb{R}$ přiřazuje číslo x^3, je bijekce množiny $\mathbb{R}$ na množinu $\mathbb{R}$.

(v) Zobrazení, které každému číslu $x \in \mathbb{R}$ přiřazuje číslo x^2, je surjekce množiny $\mathbb{R}$ na množinu všech nezáporných reálných čísel. Toto zobrazení není injekcí, a tedy ani bijekcí.

(vi) Zobrazení, které každému číslu $x \in \mathbb{R}$ přiřazuje číslo e^x, je injekce množiny $\mathbb{R}$ do množiny $\mathbb{R}$. Toto zobrazení je možno chápat jako bijekci množiny $\mathbb{R}$ na množinu všech kladných reálných čísel.

(vii) Indexovaný soubor $\{x_\alpha \ ; \ \alpha \in \Lambda\}$, kde pro každé α je $x_\alpha \in X$, není nic jiného než zobrazení množiny Λ do množiny X.

(viii) Zobrazení množiny A na množinu A, které každému prvku $a \in A$ přiřadí stejný prvek a, je bijekce. Je to tzv. *identita*, značí se většinou symbolem 1_A.

(ix) Zobrazení kartézského součinu $A \times A$ do množiny A je tzv. *binární operace* na množině A. Každým dvěma prvkům x, y množiny A je přiřazen jednoznačně určený prvek této množiny; často se označuje $x \cdot y$, xy, $x + y$ apod. Zdůrazněme, že obecně závisí na pořadí prvků x, y, tj. nemusí vždy být $x \cdot y = y \cdot x$.

Nechť f je zobrazení množiny A do množiny B.

Jestliže se prvek $a \in A$ zobrazuje na prvek $b = f(a) \in B$, pak říkáme, že je prvek b *obrazem* prvku a a prvek a *vzorem* prvku b.

Obrazem podmnožiny A' množiny A nazýváme množinu

$$f(A') = \{b \in B;\ \ \exists a \in A'\ \ b = f(a)\}\ .$$

Obraz $f(A)$ množiny A bývá rovněž označován symbolem $\operatorname{Im} f$.

Úplným vzorem podmnožiny B' množiny B nazýváme množinu

$$\{a \in A;\ \ f(a) \in B'\}\ .$$

Složením zobrazení f množiny A do množiny B a zobrazení g množiny B do množiny C dostaneme zobrazení množiny A do množiny C, které značíme gf. Velmi jednoduše lze ukázat, že složením injekcí, resp. surjekcí, resp. bijekcí je injekce, resp. surjekce, resp. bijekce. Poznamenejme, že skládání zobrazení je asociativní, tj. pro zobrazení f množiny A do množiny B, zobrazení g množiny B do množiny C a zobrazení h množiny C do množiny D je

$$h(gf) = (hg)f\ .$$

Nechť f je bijekce množiny A na množinu B. Zobrazení, které každému prvku $b \in B$ přiřazuje prvek $a \in A$, pro který je $f(a) = b$, je bijekcí množiny B na množinu A; nazývá se *inverzní zobrazení* k zobrazení f a značí se f^{-1}.

Nechť f je zobrazení množiny A do množiny B. Toto zobrazení můžeme přirozeným způsobem *zúžit* na zobrazení libovolně zvolené podmnožiny A' množiny A; získáme zobrazení f' množiny A' do množiny B, které je na množině A' definováno „stejně“ jako zobrazení f, tj.

$$\forall a \in A' \qquad f'(a) = f(a)\ .$$

Zobrazení f můžeme rovněž přirozeným způsobem *zúžit* na zobrazení množiny A do libovolné podmnožiny B'' množiny B, která obsahuje množinu $f(A)$. Toto zobrazení f'' je na množině A definováno „stejně“ jako zobrazení f, tj.

$$\forall a \in A \qquad f''(a) = f(a)\ .$$

1.3. Definice. *Relací* na množině A rozumíme každou podmnožinu ϱ kartézského součinu $A \times A$; jestliže $(x, y) \in \varrho$, pak píšeme $x \varrho y$. Relace ϱ se nazývá

– *reflexivní*, jestliže
$$\forall x \in A \qquad x \varrho x\ ;$$
– *symetrická*, jestliže
$$\forall x, y \in A \qquad x \varrho y \Longrightarrow y \varrho x\ ;$$
– *antisymetrická*, jestliže
$$\forall x, y \in A \qquad x \varrho y,\ \ y \varrho x \Longrightarrow x = y\ ;$$
– *tranzitivní*, jestliže
$$\forall x, y, z \in A \qquad x \varrho y,\ \ y \varrho z\ \Longrightarrow x \varrho z\ .$$

1.4. Definice. *Ekvivalencí* na množině A rozumíme každou relaci, která je reflexivní, symetrická a tranzitivní.

Nechť ϱ je ekvivalence na množině A. Jestliže je $x \varrho y$ (a tedy i $y \varrho x$), pak říkáme, že prvky x, y jsou *ekvivalentní*.

1.5. Definice. *Disjunktním rozkladem* množiny A budeme rozumět každý systém $\mathfrak{A}$ neprázdných podmnožin množiny A, které jsou navzájem disjunktní a jejichž sjednocením je celá množina A.

Každý prvek množiny A tedy leží právě v jediné podmnožině systému $\mathfrak{A}$.

Mezi ekvivalencemi na množině A a disjunktními rozklady této množiny existuje vzájemně jednoznačné přiřazení (bijekce).

Nechť je dána na množině A ekvivalence ϱ. Uvažujeme-li ke každému prvku $a \in A$ podmnožinu všech prvků množiny A, které jsou s ním ekvivalentní, tj. podmnožinu $\{x \in A;\ x \varrho a\}$, získáme disjunktní rozklad množiny A. Hovoříme o disjunktním rozkladu, který je určen danou ekvivalencí — příslušným podmnožinám se většinou říká *třídy ekvivalence* ϱ. Disjunktní rozklad množiny A určený ekvivalencí ϱ se většinou označuje A/ϱ (čteme „A podle ϱ“); často se též hovoří o *faktorové množině* A/ϱ množiny A podle ekvivalence ϱ.

Je-li dán disjunktní rozklad množiny A, prohlásíme za ekvivalentní ty prvky množiny A, které leží ve stejné podmnožině daného rozkladu. Hovoříme o ekvivalenci určené daným disjunktním rozkladem.

1.6. Příklady.

(i) Velmi jednoduchým příkladem ekvivalence je rovnost. Uvažujeme-li např. rovnost na množině $\mathbb{N}$ všech přirozených čísel, je odpovídajícím disjunktním rozkladem rozklad množiny $\mathbb{N}$ na jednoprvkové množiny $\{1\}$, $\{2\}$, $\{3\}$ atd.

(ii) Disjunktním rozkladem množiny $\mathbb{Z}$ je rozklad na sudá a lichá čísla

$$\mathbb{Z} = \{\ \dots\ ,\ -4,\ -2,\ 0,\ 2,\ 4,\ \dots\ \} \cup \{\ \dots\ ,\ -5,\ -3,\ -1,\ 1,\ 3,\ 5,\ \dots\ \}\ .$$

Tomuto rozkladu odpovídá ekvivalence, při které jsou navzájem ekvivalentní ta čísla, která mají stejnou *paritu*.

(iii) Zvolme pevně přirozené číslo n. Na množině $\mathbb{Z}$ uvažujme relaci $\equiv \pmod n$, která je definována takto:

$$\text{pro } a, b \in \mathbb{Z} \text{ je } a \equiv b \pmod n, \text{ jestliže pro nějaké } k \in \mathbb{Z} \text{ je } a - b = kn.$$

Např. $7 \equiv 3 \pmod 4$, $6 \equiv 71 \pmod 5$, $-3 \equiv 6 \pmod 3$. Relace $\equiv \pmod n$ je reflexivní, symetrická a tranzitivní, hovoříme o *ekvivalenci modulo* n. Čísla a, b jsou tedy ekvivalentní modulo n právě tehdy, když dávají při dělení číslem n stejný nezáporný zbytek. Např. čísla 3, 8, 18, 33, -2, -22, -37 jsou ekvivalentní modulo 5, neboť dávají při dělení číslem 5 zbytek 3.

Disjunktní rozklad množiny $\mathbb{Z}$, který odpovídá ekvivalenci $\equiv \pmod n$, neboli faktorová množina $\mathbb{Z}/\!\equiv \pmod n$ má právě n prvků; sestává z následujících podmnožin množiny $\mathbb{Z}$ (tříd ekvivalence $\equiv \pmod n$):

$$
\begin{gathered}
\{\dots,\ -4n,\ -3n,\ -2n,\ -n, 0\ ,\ n,\ 2n,\ 3n,\ 4n,\ \dots\}\ , \\
\{\dots,\ -3n+1,\ -2n+1,\ -n+1, 1\ ,\ n+1,\ 2n+1,\ 3n+1,\ \dots\}\ , \\
\{\dots,\ -3n+2,\ -2n+2,\ -n+2, 2\ ,\ n+2,\ 2n+2,\ 3n+2,\ \dots\}\ , \\
\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\
\{\dots,\ -2n-2,\ -n-2,\ -2\ ,\ n-2\ ,\ 2n-2,\ 3n-2,\ 4n-2,\ \dots\}\ , \\
\{\dots,\ -2n-1,\ -n-1,\ -1\ ,\ n-1\ ,\ 2n-1,\ 3n-1,\ 4n-3,\ \dots\}\ .
\end{gathered}
$$

Při dělení číslem n dávají všechna čísla v jednotlivých třídách po řadě nezáporné zbytky $0,\ 1,\ 2,\ \dots\ ,\ n-1$.

Faktorová množina $\mathbb{Z}/\!\equiv \pmod n$ se většinou označuje symbolem $\mathbb{Z}_n$. Její prvky, tj. výše uvedené množiny, se často značí pomocí nejmenších nezáporných čísel, která jsou v nich obsažena, např. symboly $\overline{0},\ \overline{1},\ \dots\ ,\ \overline{n-1}$. Velmi často se však pruhy vynechávají a píše se

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}\ .$$

Poznamenejme, že každá dvě celá čísla jsou ekvivalentní modulo 1, příslušný disjunktní rozklad množiny $\mathbb{Z}$ je jednoprvkový (tj. množina $\mathbb{Z}$ se vlastně „nerozloží“), $\mathbb{Z}_1 = \{0\}$. Dvě celá čísla jsou ekvivalentní modulo 2 právě tehdy, mají-li stejnou paritu; příslušný rozklad množiny $\mathbb{Z}$ je dvouprvkový (viz příklad (ii)), $\mathbb{Z}_2 = \{0, 1\}$.

Připomeňme ještě, že se místo *ekvivalence modulo n* často říká *rovnost modulo n* a místo $a \equiv b \pmod n$ se píše $a = b \pmod n$.

1.7. Definice. *Uspořádáním* na množině A rozumíme každou relaci, která je reflexivní, antisymetrická a tranzitivní. *Uspořádanou množinou* rozumíme množinu s daným uspořádáním.

Nechť A je uspořádaná množina s uspořádáním ϱ ; jestliže je $a\varrho b$ a $a \neq b$, pak říkáme, že a je *menší* než b a že b je *větší* než a.

Prvek $a \in A$ se nazývá *maximálním prvkem* množiny A, jestliže v množině A neexistuje prvek, který je větší než a, tj. jestliže

$$\forall x \in A \qquad a\varrho x \Longrightarrow x = a\ ;$$

prvek $a \in A$ se nazývá *minimálním prvkem* množiny A, jestliže v množině A neexistuje prvek, který je menší než a, tj. jestliže

$$\forall x \in A \qquad x\varrho a \Longrightarrow x = a\ .$$