SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
Fakulta elektrotechniky a informatiky

Doc. RNDr. Jana Galanová, CSc. - RNDr. Peter Kaprálik, CSc.

DISKRÉTNA
MATEMATIKA

1997

Úvod

Text obsahuje úvod z teórie množín, grafov, výrokovej logiky a booleovských funkcií. Tomuto zodpovedá aj členenie textu na kapitoly. Obrázky a tabuľky v texte sú číslované po kapitolách. Najviac pozornosti sme venovali grafom a booleovským funkciám.

K tomu, aby čitateľ zvládol cvičenia potrebuje poznať operácie s maticami, elementárne funkcie, deriváciu a integrál reálnej funkcie jednej premennej.

Publikácia je určená poslucháčom I. ročníka FEI STU v Bratislave, no môže byť učebnou pomôckou aj pre poslucháčov iných fakúlt.

Záverom si dovoľujeme poďakovať našim priateľom doc. RNDr. Ľudovítovi Niepelovi, CSc. a RNDr. Vladimírovi Janišovi, CSc. za pozorné prečítanie textu, cenné rady a pripomienky, ktoré prispeli k zlepšeniu publikácie.

Autori

Množiny

Vznik teórie množín súvisí s menami B. Bolzano (1781-1848) a G. Cantor (1845-1918). Cantor vytvoril teóriu, ktorá je základom súčasnej teórie množín.

Cantor používal intuitívny pojem množiny, ktorú považoval za „súhrn predmetov, vecí, dobre rozlíšiteľných našou mysľou alebo intuíciou". Nehovorí nič o spôsobe tvorenia množín, teda pripúšťa neobmedzenú možnosť tvorenia množín z ľubovoľných objektov. Toto viedlo k niektorým ťažkostiam - paradoxom v teórii množín. Uvedieme takýto paradox.

Podľa Cantora môžeme vytvoriť množinu, ktorej prvkami sú všetky množiny. Označme ju znakom M. Pretože M je množina, tak je aj prvkom množiny všetkých množín, teda $M \in M$. Pre množinu $\boldsymbol{N}$ všetkých prirodzených čísel zasa platí $\boldsymbol{N} \notin \boldsymbol{N}$. Rozdeľme teda množinu M všetkých množín na množiny U a V, pričom U je množina tých prvkov $X \in M$, pre ktoré platí $X \notin X$ a V je množina tých prvkov $X \in M$, pre ktoré platí $X \in X$. Platia tu tieto vzťahy:

$$M = U \cup V, \ \ U \cap V = \emptyset$$

Množiny U, V sú neprázdne, lebo $M \in V$ a $\boldsymbol{N} \in U$. Každá množina patrí do U alebo do V. Kam patrí množina U?

Ak $U \in V$, tak podľa definície V je $U \in U$. Ale, pretože $U \cap V = \emptyset$ tak, ak $U \in V$ potom $U \notin U$. Máme spor $U \in U$ a súčasne $U \notin U$. Teda nie je možné, aby $U \in V$.

Ak $U \notin V$, tak $U \in U$ a podľa definície U je $U \notin U$. Opäť máme spor.

Máme teda množinu U, ktorá nie je prvkom M, čo je v rozpore s tým, že M je množina všetkých množín. M potom ale nemôže byť množina.

Riešením tejto situácie boli pravidlá, kedy súhrn predmetov tvorí množinu. Súhrn predmetov nazývame trieda a tie triedy, z ktorých sa dajú vytvoriť ďalšie triedy, sa nazývajú množiny. Napríklad M je trieda, ktorá nie je množinou a na druhej strane všetky prirodzené čísla tvoria množinu (označme ju $\boldsymbol{N}$), lebo $\boldsymbol{N}$ je prvkom $P(\boldsymbol{N})$ množiny všetkých podmnožín množiny $\boldsymbol{N}$. V axiomatickej teórii množín sa z axiom dá dokázať, že $\boldsymbol{N}$ je množina.

Uveďme teraz označenia niektorých množín, ktoré budeme častejšie používať.

$\boldsymbol{N}$ znamená množinu všetkých prirodzených čísel, pričom aj nulu počítame medzi prirodzené čísla.
$\boldsymbol{N}^+$ znamená množinu všetkých kladných prirodzených čísel,
$\boldsymbol{Z}$ znamená množinu všetkých celých čísel,
$\boldsymbol{Q}$ znamená množinu všetkých racionálnych čísel,
$\boldsymbol{Q}^+$ znamená množinu všetkých kladných racionálnych čísel,
$\boldsymbol{R}$ znamená množinu všetkých reálnych čísel,

$\boldsymbol{R}^+$ znamená množinu všetkých kladných reálnych čísel,
(a, b) znamená otvorený interval a, b,
$\langle a, b\rangle$ znamená uzavretý interval a, b.

Mohutnosť množín

Mohutnosť množiny alebo kardinálne číslo množiny je zovšeobecnenie pojmu počet prvkov množiny. Uvedieme najskôr, kedy majú dve množiny rovnakú mohutnosť.

Množiny A, B majú ***rovnakú mohutnosť***, ak existuje bijekcia z jednej množiny na druhú. Zapisujeme to $\operatorname{card} A = \operatorname{card} B$.

Príklad.
a) Množiny $\boldsymbol{N}$ a $\boldsymbol{N}^+$ majú rovnakú mohutnosť, lebo zobrazenie $f\colon \boldsymbol{N} \to \boldsymbol{N}^+$, $f(n) = n + 1$ je bijekcia.
b) Množiny $\boldsymbol{R}$ a $\boldsymbol{R}^+$ majú rovnakú mohutnosť, lebo zobrazenie $f\colon \boldsymbol{R}^+ \to \boldsymbol{R}$, $f(x) = \ln x$ je bijekcia.
c) Množiny $A = \{0, 1, 2\}$ a $B = \{a, b, c\}$ majú rovnakú mohutnosť, lebo zobrazenie $f\colon A \to B, f(0) = a, f(1) = b, f(2) = c$ je bijekcia.
d) Intervaly $(0, 1)$ a $(-\infty, 0)$ majú rovnakú mohutnosť, lebo zobrazenie $f\colon (0, 1) \to (-\infty, 0)$, $f(x) = \ln x$ je bijekcia.
e) Interval $(1, \infty)$ a $\boldsymbol{R}^+$ majú rovnakú mohutnosť, lebo zobrazenie $f\colon (1, \infty) \to \boldsymbol{R}^+$, $f(x) = \ln x$ je bijekcia. ■

Nech $n \in \boldsymbol{N}^+$. Hovoríme, že množina A má n ***prvkov***, ak existuje bijekcia množiny $\{1, 2, ..., n\}$ na A. Prázdna množina má 0 prvkov.
Množina A sa nazýva ***konečná***, keď má k prvkov, kde k je prirodzené číslo.

Príklad. Množina $\{a, b, c, d\}$ má 4 prvky, lebo priradenie $1 \mapsto a$, $2 \mapsto b$,$3 \mapsto c$, $4 \mapsto d$, je bijekcia.
Množina $\{a_1, a_2, a_3, a_4, a_5\}$ má 5 prvkov, lebo zobrazenie $n \mapsto a_n$ je bijekcia. ■

Množina, ktorá nie je konečná, sa nazýva ***nekonečná***.

Príkladom nekonečnej množiny je množina všetkých prirodzených čísel. Toto tvrdenie nebudeme dokazovať, zoberieme to ako známy fakt. Dôkaz nájde čitateľ v každej knihe o axiomatickej teórii množín.
Nekonečné množiny ďalej delíme na spočítateľné a nespočítateľné.

Množina A sa nazýva ***spočítateľná***, keď má rovnakú mohutnosť ako množina $\boldsymbol{N}$.

Podľa definície to znamená, že musí existovať bijekcia z množiny $\boldsymbol{N}$ na A. Ak f je takáto bijekcia, tak vlastne prirodzenému číslu n priradí nejaký prvok a z množiny A, t.j. $f(n) = a$. Z matematickej analýzy poznáme aj skrátený zápis takéhoto priradenia, a to a_n. To ale znamená, že prvky množiny A sa dajú zoradiť do postupnosti. Dokázali sme tak vetu:

Veta. *Množina je spočítateľná, ak sa jej prvky dajú zoradiť do nekonečnej postupnosti.*

Príklad.
1. Množina $\boldsymbol{N}$ je spočítateľná, lebo jej prvky sa dajú zoradiť napríklad do tejto postupnosti: 0, 1, 2, 3, ...
2. Množina $\boldsymbol{N}^+$ je spočítateľná, jej prvky sa dajú zoradiť do postupnosti 1, 2, 3, 4, ...
3. Množina $\boldsymbol{Z}$ všetkých celých čísel je spočítateľná, lebo jej prvky sa dajú zoradiť do postupnosti 0, 1, -1, 2, -2, 3, -3, ... ■

Veta. *Ak dve množiny A, B sú spočítateľné, tak je spočítateľný aj ich karteziánsky súčin $A \times B$.*

Dôkaz. Prvky množiny A sa dajú zoradiť do postupnosti $a_1, a_2, a_3, a_4, ...$, prvky množiny B do postupnosti $b_1, b_2, b_3, b_4, ...$. Napíšeme si postupne prvky množiny $A \times B$, pričom využijeme zoradenie prvkov A aj B:

$$\begin{array}{llll}
(a_1,b_1), & (a_1,b_2), & (a_1,b_3), & (a_1,b_4), ... \\
(a_2,b_1), & (a_2,b_2), & (a_2,b_3), & (a_2,b_4), ... \\
(a_3,b_1), & (a_3,b_2), & (a_3,b_3), & (a_3,b_4), ... \\
(a_4,b_1), & (a_4,b_2), & (a_4,b_3), & (a_4,b_4), ... \\
\vdots & \vdots & \vdots & \vdots
\end{array}$$

Zoradíme prvky množiny $A \times B$ do postupnosti tak, že sa budeme v predchádzajúcej tabuľke pohybovať po uhlopriečkach, pričom začneme dvojicou v ľavom hornom rohu

$$(a_1,b_1), (a_2,b_1), (a_1,b_2), (a_1,b_3), (a_2,b_2), (a_3,b_1), (a_4,b_1), (a_3,b_2), (a_2,b_3), ...$$

To ale znamená, že množina $A \times B$ je spočítateľná.

Veta. *Ak množiny $A_1, A_2, A_3, ..., A_k$, $k \in \boldsymbol{N}^+$ sú spočítateľné, tak je spočítateľný aj karteziánsky súčin $A_1 \times A_2 \times ... \times A_k$.*

Dôkaz neuvedieme, robí sa indukciou vzhľadom na k, pričom prechod od k ku $k+1$ je analogický ako v predchádzajúcej vete.

Veta. *Nech A je spočítateľná množina. Potom množina B je spočítateľná práve vtedy, keď existuje bijekcia z A na B.*

Dôkaz. Ak A je spočítateľná množina, potom, podľa definície spočítateľnosti množiny, existuje bijekcia $f : A \to \boldsymbol{N}$. Potom ale $f^{-1} : \boldsymbol{N} \to A$ je tiež bijekcia.
Ak B je spočítateľná množina, tak existuje bijekcia $g : \boldsymbol{N} \to B$. Potom ale zložená funkcia $f \circ g : A \to B$ je bijekcia.

Z druhej strany, ak $h : A \to B$ je bijekcia, tak $f^{-1} \circ h : \boldsymbol{N} \to B$ je bijekcia a množina B je, podľa definície, spočítateľná.

Príklad. Nech M je množina všetkých matíc stupňa 2, tvaru $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, kde $a, b \in \boldsymbol{N}$. Množina M je spočítateľná, pretože existuje bijekcia

$$f : \boldsymbol{N} \times \boldsymbol{N} \to M,\ f(n,m) = \begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix}$$

a množina $\boldsymbol{N} \times \boldsymbol{N}$ je spočítateľná. ■

Veta. *Každá podmnožina spočítateľnej množiny je konečná alebo spočítateľná.*

Dôkaz. Nech A je spočítateľná množina a B jej podmnožina. Prvky množiny A sa dajú zoradiť do postupnosti $a_1, a_2, a_3, \ldots$. Prvky množiny B nech sa tam nachádzajú na miestach i_k, pričom počet k týchto miest je konečný alebo nekonečný. Prvky a_{i_k}, ktoré označíme $b_k = a_{i_k}$, v prvom prípade tvoria konečnú množinu, v druhom prípade sú zoradené do nekonečnej postupnosti $b_1, b_2, b_3, \ldots$. Teda B je konečná alebo spočítateľná.

Poznamenajme, že postupnosť $b_1, b_2, b_3, \ldots$ je vlastne vybraná postupnosť z postupnosti $a_1, a_2, a_3, \ldots$.

Veta. *Ak množiny A, B sú spočítateľné, tak $A \cup B$ je spočítateľná množina a $A \cap B$ je konečná alebo spočítateľná množina.*

Dôkaz. Prvky množiny A sa dajú zoradiť do postupnosti $a_1, a_2, a_3, \ldots$, prvky množiny B do postupnosti $b_1, b_2, b_3, \ldots$. Prvky množiny $A \cup B$ zoradíme do nekonečnej postupnosti $a_1, b_1, a_2, b_2, a_3, b_3, \ldots$ vtedy, keď množiny A, B sú disjunktné. Postupnosť je nekonečná, lebo množina A je nekonečná. Keď množiny A, B nie sú disjunktné, tak $A \cup B = A \cup (B - A)$ a množiny $A, B - A$ sú už disjunktné. Čiže množina $A \cup B$ je spočítateľná.
Pretože množina $A \cap B$ je podmnožinou spočítateľnej množiny A, tak je konečná alebo spočítateľná.

Veta. *Ak množina A je konečná a množina B je spočítateľná, tak množina $A \cup B$ je spočítateľná a množina $A \cap B$ je konečná.*

Dôkaz. Prvky množiny A nech sú $a_1, a_2, a_3, \ldots, a_n$, prvky množiny B sú zoradené do postupnosti $b_1, b_2, b_3, \ldots$. Všetky prvky množiny B sú prvkami množiny $A \cup B$, teda $A \cup B$ je nekonečná. Jej prvky zoradíme do postupnosti

$$a_1, a_2, \ldots, a_n, b_1, b_2, b_3, \ldots,$$

keď množiny A a B sú disjunktné. Ak nie sú, tak $A \cup B = A \cup (B - A)$, pričom množiny A, $B - A$ sú už disjunktné.

Príklad. Nech množina $A = \{-1, 1, 2, \ldots, 10\}$, množina $B = \boldsymbol{N}$ množine všetkých prirodzených čísel a množina D je množina všetkých párnych prirodzených čísel. Potom $A \cap B = \{1, 2, \ldots, 10\}$ je konečná množina a $D \cap B = D$ je nekonečná množina. ■

Veta. *Množina $\boldsymbol{Q}^+$ všetkých kladných racionálnych čísel je spočítateľná.*

Dôkaz. Prvky množiny $\boldsymbol{Q}^+$ majú tvar $\frac{p}{q}$, kde p, q sú nesúdeliteľné prirodzené čísla. Zobrazenie $f:\boldsymbol{Q}^+ \to \boldsymbol{N}^+ \times \boldsymbol{N}^+$, kde $f\left(\frac{p}{q}\right) = (p,q)$, je injektívne zobrazenie. Množina $\boldsymbol{N}^+ \times \boldsymbol{N}^+$ je spočítateľná a jej podmnožina $f(\boldsymbol{Q}^+)$ je konečná alebo spočítateľná a vzhľadom na to, že f je bijekcia $\boldsymbol{Q}^+$ na $f(\boldsymbol{Q}^+)$, tak $\boldsymbol{Q}^+$ má rovnakú mohutnosť ako $f(\boldsymbol{Q}^+)$. Pretože $\boldsymbol{Q}^+$obsahuje nekonečnú množinu $\boldsymbol{N}^+$, tak $\boldsymbol{Q}^+$je spočítateľná.

Príklad. Množina $\boldsymbol{Q}$ všetkých racionálnych čísel je spočítateľná.

Riešenie. Zobrazenie $f:\boldsymbol{Q}^+ \to \boldsymbol{Q}^-$, kde $f\left(\frac{p}{q}\right) = -\frac{p}{q}$ je bijekcia z množiny kladných racionálnych čísel $\boldsymbol{Q}^+$ na množinu všetkých záporných racionálnych čísel $\boldsymbol{Q}^-$, teda $\boldsymbol{Q}^-$ je spočítateľná množina. Potom aj množina $\boldsymbol{Q}^+ \cup \boldsymbol{Q}^-$ je spočítateľná a pridaním konečnej množiny $\{0\}$ vznikne spočítateľná množina všetkých racionálnych čísel $\boldsymbol{Q} = \{0\} \cup \boldsymbol{Q}^+ \cup \boldsymbol{Q}^-$. ■

Mohutnosťou množiny *A* nazývame symbol, priradený všetkým množinám s rovnakou mohutnosťou ako množina *A*.

Pretože pri konečných množinách existuje bijekcia iba medzi množinami s rovnakým počtom prvkov, tak sa počet prvkov používa na označenie mohutnosti konečnej množiny. Teda n-prvková množina má mohutnosť n.

Pri nekonečných množinách vzniká otázka, či všetky majú rovnakú mohutnosť ako množina $\boldsymbol{N}$, t.j. či všetky množiny sú spočítateľné. Dá sa dokázať, že napríklad otvorený interval $(0,1)$ nie je spočítateľná množina, že jeho prvky sa nedajú zoradiť do postupnosti. Preto všetky nekonečné množiny nemajú rovnakú mohutnosť. Symbol, priradený všetkým množinám s rovnakou mohutnosťou ako $\boldsymbol{N}$ je $\aleph_0$ (čítaj alef nula).

Ktoré množiny majú rovnakú mohutnosť ako interval $(0,1)$?

Príklad. Každý interval (a,b), kde a, b sú reálne čísla má rovnakú mohutnosť ako interval $(0,1)$. Funkcia $f:(0,1) \to (a,b)$, $f(x) = a + x(b-a)$, je bijekcia. ■

Príklad. Interval $(0,1)$ má rovnakú mohutnosť ako interval $(-\infty,0)$. Hľadaná bijekcia je logaritmická funkcia na $(0,1)$.

Označme $\boldsymbol{R}^- = (-\infty,0)$, $\boldsymbol{R}^+ = (0,\infty)$, $\boldsymbol{R} = (-\infty,\infty)$. Funkcia $f(x) = -x$ je bijekcia $\boldsymbol{R}^-$ na $\boldsymbol{R}^+$. Logaritmická funkcia ln je bijekcia $\boldsymbol{R}^+$ na $\boldsymbol{R}$.
Množiny $(0,1)$, $\boldsymbol{R}^-$, $\boldsymbol{R}^+$, $\boldsymbol{R}$ majú teda rovnakú mohutnosť. ■

Mohutnosť množiny $\boldsymbol{R}$ všetkých reálnych čísel označujeme *c* a nazývame ***mohutnosťou kontinua***.

Cvičenia

1. Dokážte, že všetky intervaly (a,∞), kde a je reálne číslo, majú rovnakú mohutnosť.
2. Akú mohutnosť má množina všetkých kladných racionálnych čísel? Zdôvodnite.
3. Dokážte, že množina $\{x\,; x = 5k+1, k \in \boldsymbol{N}\}$ je spočítateľná.

4. Zistite, či množina A je spočítateľná, ak

(a) $A = \{n^2;\ n \in \boldsymbol{N}\} \cup \{\frac{1}{n};\ n \in \boldsymbol{N}^+\}$,

(b) $A = \left\{ \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix};\ a,b,c,d,e \in \boldsymbol{Z} \right\}$, kde $\boldsymbol{Z}$ je množina všetkých celých čísel,

(c) $A = \bigcup\limits_{n \in \boldsymbol{N}^+} \{(x_1, x_2, ..., x_n);\ x_i \in \{0,1\}, i \in \{1,2,...,n\}\}$.

5. Zistite, či množiny A, B majú rovnakú mohutnosť, keď

(a) A je množina všetkých bodov v rovine, ktorých súradnice sú racionálne čísla a B je množina všetkých bodov na priamke, ktorých súradnice sú celé čísla.

(b) A je množina všetkých polynómov s celočíselnými koeficientami a B je množina všetkých celých čísel.

Operácie na množine

Poznáme dve základné operácie na množine $\boldsymbol{N}^+$ všetkých prirodzených čísel, a to sčítanie $+$ a násobenie $.$. Môžeme ich chápať ako funkcie f, g z množiny $\boldsymbol{N}^+ \times \boldsymbol{N}^+$ do $\boldsymbol{N}^+$, $f(x,y) = x + y$, $g(x,y) = x.y$. Takto definujeme aj operácie na ľubovoľnej množine.

Funkciu $f : A^n \to A$, $n \in \boldsymbol{N}^+$, nazývame ***n-árnou operáciou*** na množine A.
Pre $n = 1$, namiesto 1-árna operácia, hovoríme aj ***unárna*** operácia.
Pre $n = 2$, namiesto 2-árna operácia, hovoríme aj ***binárna*** operácia.
Pre $n = 3$, namiesto 3-árna operácia, hovoríme aj ***ternárna*** operácia.

Príklad. Funkcia $f(x,y) = x + y$ je binárna operácia na množine $\boldsymbol{R}$, pretože je definovaná pre každé $x, y \in \boldsymbol{R}$ a tiež $f(x,y) \in \boldsymbol{R}$.

Funkcia $g(x,y) = x.y$ je tiež binárnou operáciou na $\boldsymbol{R}$, pretože jej definičný obor je $\boldsymbol{R} \times \boldsymbol{R}$ a pre každé $x, y \in \boldsymbol{R}$ platí $g(x,y) \in \boldsymbol{R}$.

Funkcia $h(x,y) = x - y$ je binárna operácia na $\boldsymbol{R}$, pretože pre každé $x, y \in \boldsymbol{R}$ platí $x - y \in \boldsymbol{R}$.

Funkcia $k(x) = x + 3$ je unárna operácia na $\boldsymbol{R}$, pretože pre každé $x \in \boldsymbol{R}$ platí $x + 3 \in \boldsymbol{R}$.

Funkcia $t(x,y) = \frac{x}{y}$ nie je operácia na $\boldsymbol{R}$, pretože nie je definovaná pre $y = 0, 0 \in \boldsymbol{R}$, teda jej definičný obor nie je celé $\boldsymbol{R} \times \boldsymbol{R}$. ■

Príklad. Funkcia $f(x,y) = x + y$ je binárna operácia na $\boldsymbol{R}^+$, množine všetkých kladných reálnych čísel, lebo súčet každých dvoch kladných reálnych čísel je kladné reálne číslo.

Taktiež súčin každých dvoch kladných reálnych čísel je kladné reálne číslo, teda súčin je binárna operácia na $\boldsymbol{R}^+$.

Rozdiel každých dvoch kladných reálnych čísel nemusí byť kladné reálne číslo, napr. $2 - 3 = -1 \notin \boldsymbol{R}^+$, pričom $2, 3 \in \boldsymbol{R}^+$, teda rozdiel nie je binárna operácia na množine $\boldsymbol{R}^+$.

Ternárnou operáciou na $\boldsymbol{R}^+$ je $g(x,y,z) = (x + y).z$, lebo pre každé tri kladné reálne čísla x, y, z je súčet $x + y = t \in \boldsymbol{R}^+$, aj súčin $t.z \in \boldsymbol{R}^+$. ■

Príklad. Označme $M_{n \times m}$ množinu všetkých matíc typu $n \times m$ nad množinou $\boldsymbol{R}$ všetkých reálnych čísel. Potom sčítanie matíc je binárna operácia na $M_{n \times m}$, lebo súčet každých dvoch matíc s reálnymi koeficientami typu $n \times m$ je zasa matica typu $n \times m$ s reálnymi koeficientami.

Násobenie matíc z $M_{n\times m}$ je definované len vtedy, keď $n = m$ a vtedy súčin matíc s reálnymi koeficientami stupňa n je zasa matica stupňa n s reálnymi koeficientami. To znamená, že násobenie je binárna operácia na $M_{n\times n}$. Násobenie nie je binárna operácia na $M_{n\times m}$, $n \neq m$. ■

Príklad. Nech M je množina všetkých regulárnych matíc stupňa 2 nad $\boldsymbol{R}$. Potom násobenie matíc je binárna operácia na M, lebo súčin regulárnych matíc nad $\boldsymbol{R}$ je regulárna matica nad $\boldsymbol{R}$. Pripomeňme, že regulárna matica je taká, ktorej determinant je rôzny od nuly.

Funkcia $f(X)$, ktorá každej matici X z M priradí determinant matice X, nie je unárna operácia na M, lebo $f(X) \notin M$, je to číslo a nie matica stupňa 2. ■

Binárna operácia f na množine A sa nazýva ***komutatívna***, keď pre každé $x, y \in A$ platí

$$f(x,y) = f(y,x) \qquad \text{(komutatívny zákon)}$$

Binárna operácia f na množine A sa nazýva ***asociatívna***, ak pre každé $x, y, z \in A$ platí

$$f(f(x,y),z) = f(x,f(y,z)) \qquad \text{(asociatívny zákon)}$$

Prvok $e \in A$ sa nazýva ***neutrálny prvok (alebo jednotkový prvok)*** binárnej operácie f na A, ak pre každé $x \in A$ platí $f(e,x) = f(x,e) = x$.

Prvok $o \in A$ sa nazýva ***nulový prvok*** binárnej operácie f na A, ak pre každé $x \in A$ platí $f(o,x) = f(x,o) = o$.

Poznamenajme, že napr. asociatívny zákon je v uvedenej forme málo podobný napríklad na asociatívny zákon známy z násobenia reálnych čísel

$$(x.y).z = x.(y.z).$$

Preto sa obvykle používa namiesto znaku f pre binárnu operáciu na množine znak ., alebo •, resp. iný znak v tvare krúžku. Prepíšme predchádzajúce zákony pomocou znaku . :

komutatívnosť:	$x.y = y.x$,
asociatívnosť:	$(x.y).z = x.(y.z)$,
neutrálny prvok:	$x.e = e.x = x$,
nulový prvok:	$o.x = x.o = o$.

Príklad. Binárna operácia sčítania (+) na množine $\boldsymbol{R}$ je
asociatívna, lebo pre každé $x, y, z \in \boldsymbol{R}$ platí $(x+y)+z = x+(y+z)$,
komutatívna, lebo pre každé $x, y \in \boldsymbol{R}$ platí $x+y = y+x$.
Neutrálnym prvkom pre + je číslo nula, lebo $0 \in \boldsymbol{R}$ a pre každé $x \in \boldsymbol{R}$ platí $x+0 = 0+x = x$.
Nulový prvok pre + neexistuje, lebo zo vzťahu $x+o = o$ vyplýva, že $x = 0$, teda vzťah neplatí pre všetky $x \in \boldsymbol{R}$.

Binárna operácia násobenia (.) na množine $\boldsymbol{R}$ je
asociatívna, lebo pre každé $x, y, z \in \boldsymbol{R}$ platí $(x.y).z = x.(y.z)$,
komutatívna, lebo pre každé $x, y \in \boldsymbol{R}$ platí $x.y = y.x$.

Neutrálnym (jednotkovým) prvkom pre násobenie je číslo jedna, lebo $1 \in \boldsymbol{R}$ a pre každé $x \in \boldsymbol{R}$ platí $x.1 = 1.x = x$. Nulovým prvkom je číslo nula, lebo $0 \in \boldsymbol{R}$ a pre každé $x \in \boldsymbol{R}$ platí $0.x = x.0 = 0$. ■

Príklad. Nech M je množina všetkých matíc stupňa 2 nad $\boldsymbol{R}$. Nech $X, Y, Z \in M$, $O \in M$ je nulová matica $O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, a $I \in M$ je jednotková matica $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Potom, ako vieme z lineárnej algebry, platí:

Binárna operácia (+) sčítavania matíc na M je
komutatívna, t.j. $X + Y = Y + X$,
asociatívna, t.j. $(X + Y) + Z = X + (Y + Z)$.

Binárna operácia (.) násobenia matíc na M
je asociatívna, t.j. platí $(X.Y).Z = X.(Y.Z)$,
nie je komutatívna, lebo napríklad pre matice

$$X = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}, \ Y = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \text{ je } X.Y = \begin{pmatrix} 3 & 3 \\ 4 & 4 \end{pmatrix}, \ Y.X = \begin{pmatrix} 3 & 4 \\ 3 & 4 \end{pmatrix},$$

teda $X.Y \neq Y.X$. Nulová matica O je neutrálny prvok pre operáciu sčítavania, lebo platí $X + O = O + X = X$, jednotková matica I je neutrálny prvok pre operáciu násobenia, lebo platí $X.I = I.X = X$. ■

Veta. *Zákony asociatívny a komutatívny sú nezávislé, t.j. jeden nevyplýva z druhého.*

Dôkaz. Stačí nájsť binárnu operáciu f na nejakej množine A, ktorá je asociatívna a nie je komutatívna a binárnu operáciu g na množine B, ktorá je komutatívna a nie je asociatívna.

Stačí zobrať za A množinu všetkých matíc stupňa 2 a za f násobenie matíc. Z predchádzajúceho príkladu vidno, že násobenie je asociatívne, ale nie je komutatívne.

Za g zoberieme binárnu operáciu $x \bullet y = \frac{1}{2}(x + y)$ na množine $\boldsymbol{R}$. Pretože operácia + na $\boldsymbol{R}$ je komutatívna, tak aj $\bullet$ je komutatívna. Skúmajme platnosť asociatívneho zákona $x \bullet (y \bullet z) = (x \bullet y) \bullet z$. Pretože

$$x \bullet (y \bullet z) = \tfrac{1}{2}(x + (y \bullet z)) = \tfrac{1}{2}(x + \tfrac{1}{2}(y + z)) = \tfrac{x}{2} + \tfrac{y}{4} + \tfrac{z}{4},$$

$$(x \bullet y) \bullet z = (\tfrac{1}{2}(x + y) \bullet z) = \tfrac{1}{2}(\tfrac{x+y}{2} + z) = \tfrac{x}{4} + \tfrac{y}{4} + \tfrac{z}{2},$$

tak pre $x = 1, y = 0, z = 2$ nie je pravda, že $1 \bullet (0 \bullet 2) = (1 \bullet 0) \bullet 2$, teda $\bullet$ nie je asociatívna operácia. 🔔

Cvičenia

1. Keď $f(x, y) = \frac{x}{y}$, množina $A = \boldsymbol{R} - \{0\}$, tak zistite, či
a) f je binárna operácia na A,
b) f je komutatívna,
c) f je asociatívna,
d) existuje neutrálny prvok a nulový prvok pre f.

2. Zistite, či f je binárna operácia na množine A, či je komutatívna, či je asociatívna, či má neutrálny prvok a nulový prvok, ak

a) $f(x,y)=x.y,\ A=\boldsymbol{R}-\{0\}$,
b) $f(x,y)=x+y,\ A=\boldsymbol{R}-\{0\}$,
c) $f(x,y)=x^y,\ A=\boldsymbol{R}^+$,
d) $f(x,y)=x.y,\ A=\{0,1\}$,
e) $f(x,y)=x+y-1,\ A=\boldsymbol{R}$,
f) $f(x,y)=x-y,\ A=\boldsymbol{R}$,
g) $f(x,y)=2x+3y,\ A=\boldsymbol{N}$,
h) $f(\overline{x},\overline{y})=\overline{x}+\overline{y},\ A$ je množina všetkých dvojrozmerných vektorov,
i) $f(X,Y)$ je stred úsečky s koncovými bodmi X, Y a A je množina všetkých bodov v rovine.

3. Nech A je množina všetkých diferencovateľných funkcií $F:\boldsymbol{R}\to\boldsymbol{R}$. Zistite, či f je unárna operácia na A, keď
a) $f(F)=F'$, kde F' je derivácia funkcie F,
b) $f(F)=\int F$, kde $\int F$ je neurčitý integrál z F,
c) $f(F)=2F+3$,
d) $f(F)=F+\sin$, pričom sin znamená funkciu sinus.

4. Nech $f(F)=X^{-1}$, kde X^{-1} je inverzná matica k matici X a $g(X,Y)=Y.X$ je súčin matíc. Zistite, či f je unárna a g binárna operácia na množine A, keď
a) A je množina všetkých matíc stupňa 2 nad $\boldsymbol{R}$,
b) A je množina všetkých regulárnych matíc stupňa 2 nad $\boldsymbol{R}$,
c) A je množina pozostávajúca z jednotkovej matice stupňa 2 nad $\boldsymbol{R}$ a nulovej matice stupňa 2 nad $\boldsymbol{R}$,
d) A je množina všetkých jednotkových matíc nad $\boldsymbol{R}$.

Relácie na množine

V tejto časti budeme hovoriť o reláciách na množine A. A^n znamená karteziánsky súčin $A\times A\times\cdots\times A$, kde množina A sa nachádza n-krát. Prvky A^n sú n-tice $(a_1,a_2,\ldots,a_n)$. Definujeme dva význačné typy binárnych relácií a to ekvivalenciu na množine a čiastočné usporiadanie na množine. Relácia ekvivalencie je dôležitá aj preto, lebo pri splnení ďalších vlastností umožňuje prenášať operácie (napr. súčty, súčiny) z prvkov množiny na celé bloky, t.j. podmnožiny danej množiny.

Podmnožinu karteziánskeho súčinu $A^n, n\in N^+$ nazývame ***n-árnou reláciou na množine** A*.

Poznámka. Namiesto 1-árna relácia hovoríme unárna relácia, namiesto 2-árna relácia hovoríme binárna relácia a namiesto 3-árna relácia hovoríme ternárna relácia.

Príklad. Nech $A=\boldsymbol{N}$. Potom
$P=\{(n,n+1);n\in\boldsymbol{N}\}$ je binárna relácia na $\boldsymbol{N}$,

$Q = \{(n^2, n, 1); n \in \boldsymbol{N}\}$ je ternárna relácia na $\boldsymbol{N}$,
S - podmnožina všetkých párnych čísel je unárna relácia na $\boldsymbol{N}$. ■

Ak $P \subset A^2$ je binárna relácia na A a $(a,b) \in P$, tak hovoríme, že *a* ***je v relácii*** *P* s b. Namiesto $(a,b) \in P$ píšeme aj aPb.

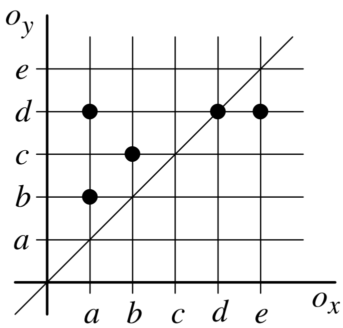
Príklad. Nech $m \in \boldsymbol{N}^+$ je pevne dané číslo. Definujme binárnu reláciu P na množine $\boldsymbol{Z}$ všetkých celých čísel takto: $P = \{(x,y); y - x = km, k \in \boldsymbol{Z}\}$. Túto reláciu je zvykom označovať $\operatorname{mod} m$ (čítaj modulo m). Ktoré prvky sú v relácii s celým číslom 1? Sú to také prvky y, pre ktoré platí $y = 1 + km$, $k \in \boldsymbol{Z}$, teda prvky $1, 1+m, 1-m, 1+2m, 1-2m, \ldots$. Napríklad pre $m = 2$ s prvkom 1 sú v relácii prvky 1, 3, –1, 5, – 3, 7, ... S prvkom 2 sú v relácii prvky 2, 4, 0, 6, –2,... . ■

Ďalej sa budeme zaoberať binárnymi reláciami na množine. Binárnej relácii $P \subset A^2$, kde A je konečná množina, priraďujeme graf relácie a tiež orientovaný graf relácie.

Graf relácie je analógiou grafu reálnej funkcie jednej reálnej premennej, pričom na súradnicové osi sa symbolicky nakreslia prvky množiny A. Presnejšie:

Nech $P \subset A^2$ a nech $f: A \to \boldsymbol{R}$, kde $\boldsymbol{R}$ je množina všetkých reálnych čísel, je injektívna funkcia, pričom body na súradnicových osiach namiesto $f(a)$ označíme a, pre $a \in A$. V rovine potom vyznačíme všetky body $(a,b) \in P$. Túto množinu bodov nazývame ***graf relácie P***.

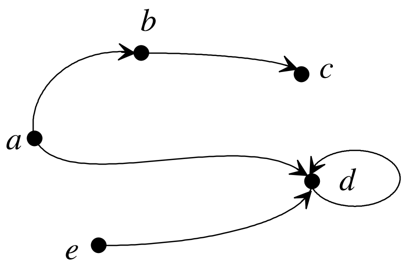
Príklad. Nech $A = \{a,b,c,d,e\}$ a nech $P = \{(a,b),(b,c),(a,d),(d,d),(e,d)\}$ je binárna relácia na A. Nakreslíme graf relácie P. Ako je zvykom, budeme súradnicové osi označovať o_x a o_y.



Obr. 1 ■

Pri orientovanom grafe relácie ide o graf v ponímaní teórie grafov. Ak P je binárna relácia na množine A, postupujeme takto: Prvkom množiny A injektívne priradíme body roviny a keď $(a,b) \in P$, tak vedieme od a k b orientovanú čiaru. Keď toto vykonáme pre všetky dvojice $(a,b) \in P$, tak dostaneme orientovaný graf relácie P.

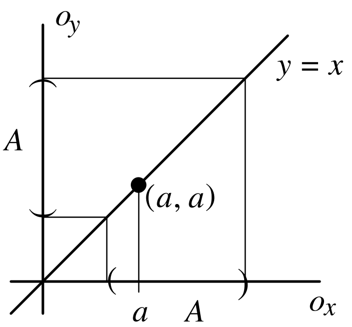
Príklad. Nakreslime orientovaný graf binárnej relácie P z predchádzajúceho príkladu.



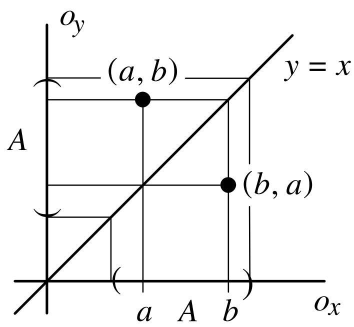
Obr. 2 ■

Binárna relácia P na množine A sa nazýva
reflexívna, ak pre každé $a \in A$ platí aPa,
symetrická, ak z platnosti aPb vyplýva bPa,
antisymetrická, ak z platnosti aPb a zároveň bPa vyplýva $a = b$,
tranzitívna, ak z platnosti aPb a zároveň bPc vyplýva aPc.

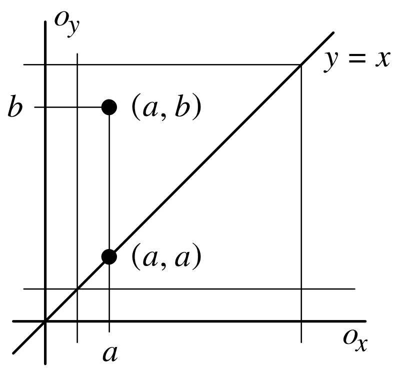
Ukážeme si, ako sa tieto vlastnosti prejavia na grafe a orientovanom grafe binárnej relácie.



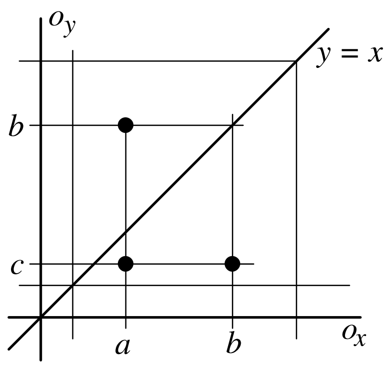
Obr. 3. Reflexívnosť:
Všetky body uhlopriečky
patria do relácie.



Obr. 4. Symetrickosť:
Graf je symetrický vzhľadom
na priamku $y = x$.

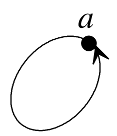


Obr. 5. Antisymetrickosť:
Graf neobsahuje žiadne body
symetrické vzhľadom na priamku
$y = x$, okrem bodov priamky $y = x$.

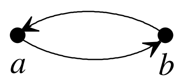


Obr. 6. Tranzitívnosť:
Graf musí byť dostatočne plný,
t.j. ak $(a, b), (b, c)$ je z grafu,
tak aj (a, c) je z grafu.

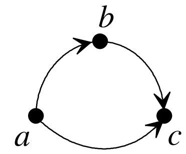
Pri orientovanom grafe:



Obr.7. Reflexívnosť: Z každého bodu a vedie orientovaná čiara do a.



Obr.8. Symetrickosť: Ak vedie orientovaná čiara z a do b, tak aj z b do a.



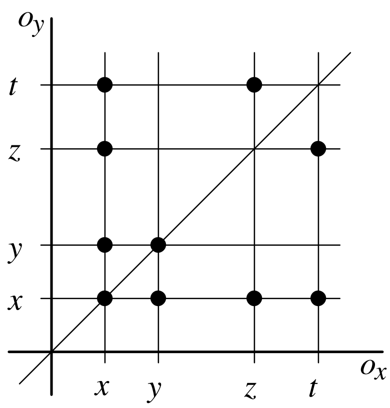
Obr.9. Tranzitívnosť: Ak vedie orientovaná čiara z a do b a z b do c, tak aj z a do c.

Antisymetria: Nemôže nastať situácia z obr. 8, iba v prípade $a = b$.

Príklad. Nech $A = \{x, y, z, t\}$ a relácia P je definovaná takto:

$$P = \{(x,z),(x,y),(x,x),(y,y),(z,x),(y,x),(z,t),(t,z),(x,t),(t,x)\}.$$

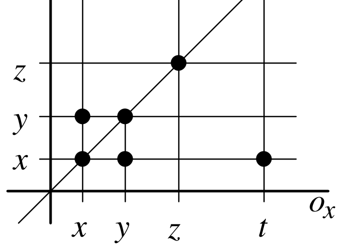
Nakreslíme graf relácie.



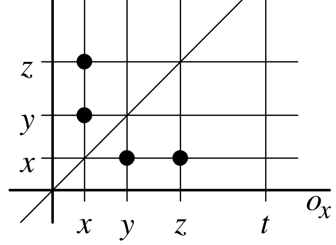
Obr. 10

Relácia nie je reflexívna, lebo napr. $(z,z) \notin P$. Relácia je symetrická, lebo jej graf je symetrický vzhľadom na priamku $y = x$. Relácia nie je antisymetrická, lebo napríklad $(x,y) \in P$, aj $(y,x) \in P$. Relácia nie je tranzitívna, lebo $(y,x),(x,z) \in P$, ale (y,z) nepatrí do P. ■

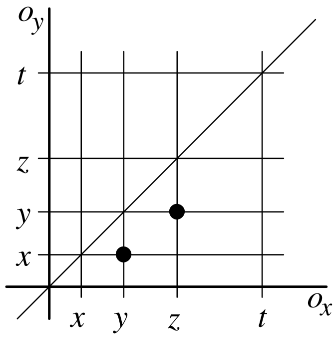
Nakreslíme postupne grafy relácií, ktoré majú vždy iba jednu z vlastností: reflexívnosť, symetrickosť, antisymetrickosť, alebo tranzitívnosť.



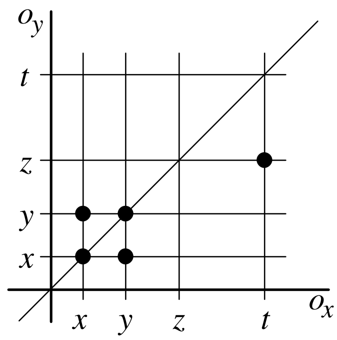
Obr. 11. Relácia je len reflexívna.



Obr. 12. Relácia je len symetrická.



Obr. 13. Relácia je len antisymetrická.



Obr. 14. Relácia je len tranzitívna.

Príklad. Zistite, či relácia $P \subset \boldsymbol{R}^2, P = \{(x,y); x \le y\}$ je reflexívna, symetrická, antisymetrická, tranzitívna.

Riešenie. Relácia je reflexívna, lebo pre každé $x \in \boldsymbol{R}$ platí $x \le x$, t.j. xPx.
Relácia nie je symetrická, pretože napríklad $2P3$ platí, ale $3P2$ neplatí.
Relácia je antisymetrická: Nech xPy, yPx, teda $x \le y, y \le x$. Z vlastností reálnych čísel vieme, že potom platí $x = y$.
Relácia je tranzitívna: Ak xPy a zároveň yPz, teda $x \le y$ a zároveň $y \le z$, potom z vlastností reálnych čísel vyplýva platnosť $x \le z$, teda xPz. ■

Príklad. Dokážte, že relácia $P = \operatorname{mod} m$ na množine $\boldsymbol{Z}$ je reflexívna, symetrická, tranzitívna.

Riešenie. Reflexívnosť: Pre každé celé číslo z platí $x - x = k \,.\, m$ pre $k = 0$, čo znamená xPx.
Symetrickosť: Ak xPy, tak $y - x = k \,.\, m$, pre nejaké celé číslo k, ale potom aj $x - y = (-k) \,.\, m$, pre celé číslo $-k$, teda yPx.
Tranzitívnosť: Ak platí xPy aj yPz, t.j. $y - x = k \,.\, m$, $z - y = l \,.\, m$, kde k, l sú celé čísla, tak $z - x = z - y + y - x = (k + l) \,.\, m$, kde $k + l \in \boldsymbol{Z}$, teda xPz. ■

Veta. *Ak relácia $P \subset A^2$ je zároveň symetrická aj antisymetrická, tak $P \subset \{(a,a); a \in A\}$.*

Dôkaz. Ak relácia P je symetrická, tak z aPb vyplýva aj bPa. Relácia je aj antisymetrická, potom ale z aPb, bPa vyplýva $a = b$, čo sme mali dokázať. 🔔

Ekvivalencia na množine

Binárna relácia na množine A, ktorá je reflexívna, symetrická a tranzitívna, sa nazýva ***ekvivalencia*** alebo ***relácia ekvivalencie*** na množine A.

Poznámka. Ak P je relácia ekvivalencie na množine A, tak okrem označenia $(a,b) \in P$, resp. aPb, sa používa aj označenie $a \equiv b(P)$.

Príklad. Relácia $\bmod m$ na množine $\mathbf{Z}$ celých čísel je podľa predchádzajúceho príkladu ekvivalencia na $\mathbf{Z}$. ■

Príklad. Nech A je množina všetkých priamok v rovine. Nech P je relácia rovnobežnosti priamok, t.j. pre priamky $p, q \in A$ platí pPq práve keď p je rovnobežná s q. Overme si, že relácia rovnobežnosti na A je ekvivalencia na A.

Riešenie. Nech p, q, r sú priamky v rovine.

Relácia P je reflexívna, lebo p je rovnobežná sama so sebou, t.j. pPp.

Relácia je symetrická, pretože z podmienky pPq, teda p je rovnobežná s q, vyplýva aj q je rovnobežná s p, t.j. qPp.

Relácia je tranzitívna, lebo ak p je rovnobežná s q a q je rovnobežná s r, tak aj p je rovnobežná s r. ■

Príklad. Relácia P rovnosti na množine A, $P = \{(a,b) \in A^2; a = b\}$ je ekvivalencia na množine A. Pretože iba $(a,a) \in P$, $a \in A$, je zrejmá reflexívnosť, symetrickosť aj tranzitívnosť relácie. ■

Veta. *Ak P a Q sú relácie ekvivalencie na množine A, tak $P \cap Q$ je relácia ekvivalancie na množine A, $P \cup Q$ nemusí byť reláciou ekvivalencie na množine A.*

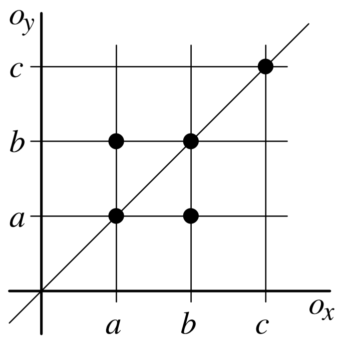
Dôkaz. Reflexívnosť $P \cap Q$: Pre každé $a \in A$ platí $(a,a) \in P$, $(a,a) \in Q$, teda $(a,a) \in P \cap Q$.

Symetrickosť $P \cap Q$: Ak $(a,b) \in P \cap Q$, tak $(a,b) \in P$ aj $(a,b) \in Q$. Pretože P, Q sú symetrické relácie, tak platí $(b,a) \in P$, $(b,a) \in Q$. To znamená, že $(b,a) \in P \cap Q$.

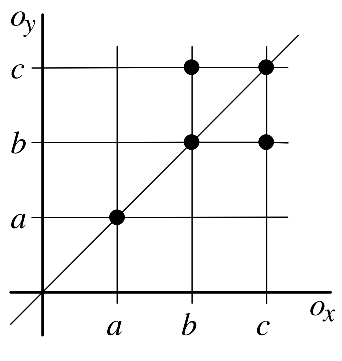
Tranzitívnosť $P \cap Q$: Nech $(a,b) \in P \cap Q$, $(b,c) \in P \cap Q$, tak $(a,b) \in P, (b,c) \in P$, ale aj $(a,b) \in Q$, $(b,c) \in Q$. Z tranzitívnosti relácií P, Q vyplýva, že aj $(a,c) \in P$, aj $(a,c) \in Q$, čiže $(a,c) \in P \cap Q$.

Dokázali sme, že $P \cap Q$ je ekvivalencia na A. Na dôkaz druhej časti vety stačí uviesť príklad, kedy $P \cup Q$ nebude ekvivalencia na A a P, Q budú ekvivalencie na množine A.

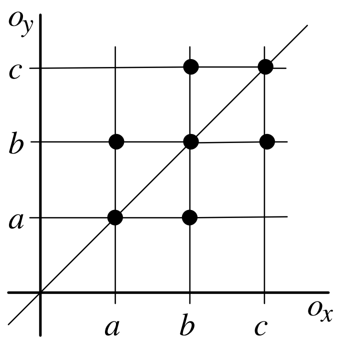
Nech $A = \{a,b,c\}$, $P = \{(a,a),(b,b),(c,c),(a,b),(b,a)\}$ a nech $Q = \{(a,a),(b,b),(c,c),(b,c),(c,b)\}$. Nakreslíme ich grafy.



Obr. 15. Graf relácie P



Obr. 16. Graf relácie Q



Obr. 17. Graf relácie $P \cup Q$

Relácia $P \cup Q$ nie je tranzitívna, lebo napríklad $(a,b) \in P \cup Q$, $(b,c) \in P \cup Q$, ale $(a,c) \notin P \cup Q$. Tým je dôkaz skončený. 🔔

Poznamenajme, že zjednotenie ekvivalencií *P, Q* je relácia, ktorá je reflexívna aj symetrická, ale nemusí byť tranzitívna, ako sme videli v dôkaze predchádzajúcej vety.

Nech P je relácia $\bmod 3$ na množine celých čísel $\mathbf{Z}$. Vytvorme množiny tých prvkov, ktoré sú v relácii P postupne s prvkom 0, prvkom 1, prvkom 2. Označme ich postupne $P(0), P(1), P(2)$. Teda pre $a \in \{0,1,2\}$ platí

$$P(a) = \{y \in \mathbf{Z}; (a,y) \in P\} = \{y \in \mathbf{Z}; y - a = k\,.\,3, k \in \mathbf{Z}\}.$$

$\mathbf{Z}$ je spočítateľná množina, zoradíme jej prvky do postupnosti

$$\mathbf{Z} = \{0, 1, -1, 2, -2, ...\}.$$

V tomto poradí budeme dosadzovať za čísla k z definície $P(a)$.

$$P(0) = \{y \in Z; y = 3k,\ k \in \mathbf{Z}\} = \{0, 3, -3, 6, -6, ...\}$$

$$P(1) = \{y \in Z; y = 3k+1,\ k \in \mathbf{Z}\} = \{1, 4, -2, 7, -5, ...\}$$

$$P(2) = \{y \in Z; y = 3k+2,\ k \in \mathbf{Z}\} = \{2, 5, -1, 8, -4, ...\}$$

Vidíme, že $P(0) \cap P(1) = \emptyset$, $P(0) \cap P(2) = \emptyset$, $P(1) \cap P(2) = \emptyset$. Táto vlastnosť je zrejmá aj z toho, že v $P(0)$ sú všetky celé čísla deliteľné tromi, t.j. tie, ktorých zvyšok po delení tromi je 0, v $P(1)$ tie, kde zvyšok po delení tromi je 1 a v $P(2)$ tie, kde zvyšok po delení tromi je 2. Vieme, že zvyšky po delení číslom 3 sú iba 0, 1, 2, teda $P(0) \cup P(1) \cup P(2) = \mathbf{Z}$.

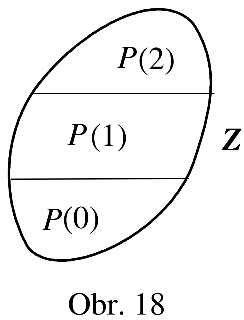
Aký tvar bude mať $P(b)$, $b \neq 0, 1, 2$? Napíšme b v tvare $b = 3l + r$, kde r je zvyšok po delení čísla b číslom 3, $0 \le r \le 3$. Potom

$$P(b) = \{y \in \mathbf{Z}; (b,y) \in P\} = \{y \in \mathbf{Z}; y = b + 3k,\ k \in \mathbf{Z}\} =$$
$$= \{y \in \mathbf{Z}; y = 3(k+l) + r\}$$

Množina $P(b)$je teda množina tých celých čísel, ktoré majú zvyšok r po delení číslom 3, teda je to $P(0)$ alebo $P(1)$ alebo $P(2)$. Napríklad

$$P(3) = P(0),\ P(8) = P(2),\ P(10) = P(1)$$

Máme teda nasledovnú situáciu: Alebo $P(x) = P(y)$, alebo $P(x) \cap P(y) = \emptyset$ pre ľubovoľné $x, y \in \mathbf{Z}$ (obr. 18).



Obr. 18

Množinu $P(x)$ nazývame triedou ekvivalencie $\bmod 3$ k prvku x. Zistili sme, že triedy ekvivalencie k dvom rôznym prvkom *x, y* sa alebo rovnajú, alebo sú disjunktné.

Takáto situácia nastáva všeobecne pre každú reláciu ekvivalencie na množine. Dokážeme to.

Nech P je relácia ekvivalencie na množine A a $x \in A$. Potom množinu $P(x) = \{y \in A; xPy\}$ nazývame ***triedou ekvivalencie*** k prvku x.

Veta. (O triedach ekvivalencie). *Nech P je relácia ekvivalencie na množine A a nech $a, b \in A$. Potom pre triedy ekvivalencie $P(a)$* a *$P(b)$ k prvkom a, b platí: $P(a) = P(b)$ alebo $P(a) \cap P(b) = \emptyset$.*

Dôkaz. Prienik dvoch množín je prázdny alebo neprázdny. Nech $P(a) \cap P(b) \neq \emptyset$. Chceme dokázať, že vtedy $P(a) = P(b)$.

Nech $c \in P(a) \cap P(b)$. Potom platí aPc, bPc. Ak $s \in P(a)$, tak aPs. Využijeme platnosť aPc, zo symetrickosti relácie P platí aj cPa a keď použijeme tranzitívnosť P na cPa, aPs, tak máme cPs. Opätovné využitie tranzitívnosti P na bPc, cPs dáva platnosť vzťahu bPs, čiže $s \in P(b)$. Ukázali sme, že $P(a)$ je podmnožina $P(b)$.

Zámenou množín $P(a)$ a $P(b)$ dokážeme, že aj $P(b)$ je podmnožinou $P(a)$. Spolu potom platí $P(a) = P(b)$. Veta je dokázaná. 🕭

Príklad. Už sme ukázali, že relácia P rovnobežnosti priamok v rovine je reláciou ekvivalencie na množine A všetkých priamok v rovine. Nájdime triedy ekvivalencie k priamkam p a q, kde $p: y = 2x + 1$, $q: x = 2$.

Riešenie. Podľa definície $P(p) = \{p_1 \in A;\ pPp_1\}$. Priamka p má smernicu 2, tak p_1 je daná rovnicou $y = 2x + b$, kde $b \in \boldsymbol{R}$. Túto triedu ekvivalencie charakterizuje jednoznačne smernica priamky.

Priamka q nemá smernicu, je rovnobežná s osou y-ovou v rovine. Teda práve všetky priamky rovnobežné s osou y-ovou budú tvoriť jednu triedu a to je trieda $P(q)$. ■

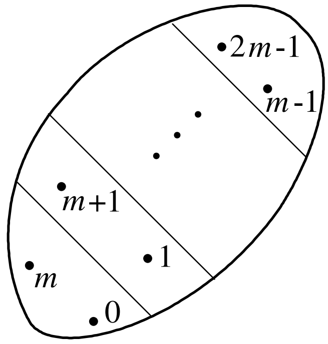
Rozkladom množiny A nazývame systém podmnožín $A_i \subset A, i \in I$ taký, že $\bigcup_{i \in I} A_i = A$, $A_i \cap A_j = \emptyset$ pre $i \neq j$, kde $i, j \in I$. Množiny $A_i, i \in I$ sa nazývajú ***triedy rozkladu***.

Príklad. Množiny A_1, A_2, kde A_1 je množina všetkých nepárnych čísel, A_2 je množina všetkých párnych čísel, tvoria rozklad množiny $\boldsymbol{N}$, pretože platí $A_1 \cup A_2 = \boldsymbol{N}$ a $A_1 \cap A_2 = \emptyset$. Tento rozklad má dve triedy rozkladu, a to A_1 a A_2. ■

Veta. *Nech P je ekvivalevcia na množine A. Potom triedy ekvivalencie $P(a)$, $a \in A$ tvoria rozklad množiny A. Triedami rozkladu sú triedy ekvivalencie P.*

Dôkaz. Podľa vety o triedach ekvivalencie, ak sú triedy ekvivalencie $P(x), P(y)$ rôzne, tak sú disjunktné. Máme dokázať, že ich zjednotením je množina A, t.j. každý prvok $a \in A$ sa nachádza v niektorej z tried ekvivalencie P. Pretože P je reflexívna, tak aPa, teda $a \in P(a)$. To znamená, že triedy ekvivalencie tvoria rozklad množiny A a teda sú aj triedami tohto rozkladu. 🕭

Príklad. Relácia mod$m$ na množine $\boldsymbol{Z}$ všetkých celých čísel má m rôznych tried ekvivalencie, a to $P(0), P(1), ..., P(m-1)$. Pre jednoduchosť ich označme $\overline{0}, \overline{1}, ..., \overline{m-1}$. Systém podmnožín $\overline{0}, \overline{1}, ..., \overline{m-1}$ je rozklad množiny $\boldsymbol{Z}$ a má m tried rozkladu. ■



Obr. 19. Triedy rozkladu mod m

Príklad. Relácia P rovnobežnosti priamok v rovine je ekvivalencia. Určuje rozklad množiny všetkých priamok na triedy ekvivalencie. Jednu triedu rozkladu tvoria všetky priamky bez smernice. V každej ďalšej triede rozkladu sú priamky so smernicou. Všetky rovnobežné priamky majú rovnakú smernicu a teda smernica jednoznačne charakterizuje triedu ekvivalencie. Rôzne smernice charakterizujú rôzne triedy ekvivalencie a keďže smernice tvoria nespočítateľnú množinu $\boldsymbol{R}$, tak aj triedy ekvivalencie tvoria nespočítateľnú množinu. ■

Veta. *Nech množiny $A_i, i \in I$ tvoria rozklad množiny A. Týmto rozkladom je jednoznačne určená ekvivalencia na A taká, že triedy rozkladu sú triedami ekvivalencie.*

Dôkaz. Na množine A definujeme reláciu P takto:

$$aPb \text{ práve keď } a, b \in A_i \text{ pre niektoré } i \in I.$$

Táto relácia je reflexívna, lebo pre každé $a \in A$, kde $A = \bigcup_{i \in I} A_i$, platí $a \in A_i$ pre niektoré $i \in I$.
Relácia je symetrická, lebo z platnosti aPb vyplýva $a, b \in A_i$ pre nejaké $i \in I$, teda aj $b, a \in A_i$, čo znamená bPa.
Relácia je tranzitívna, lebo ak aPb aj bPc, tak pre nejaké $i, j \in I$ platí $a, b \in A_i$, $b, c \in A_j$. Pretože $b \in A_i \cap A_j$, tak z definície rozkladu vyplýva $i = j$. Potom ale aj $a, c \in A_i$, teda aPc.

Dokázali sme, že P je ekvivalencia. To, že triedy rozkladu sú triedami tejto ekvivalencie je evidentné z definície relácie P. 🔔

Príklad. Najdite na množine $A = \{1, 2, ..., 10\}$ dve rôzne relácie ekvivalencie.

Riešenie. Urobme dva rôzne rozklady množiny A. Prvý rozklad A má dve triedy rozkladu, a to

$$A_1 = \{1, 2, 3, 4\},\ A_2 = \{5, 6, 7, 8, 9, 10\}$$

Druhý rozklad má štyri triedy rozkladu, a to

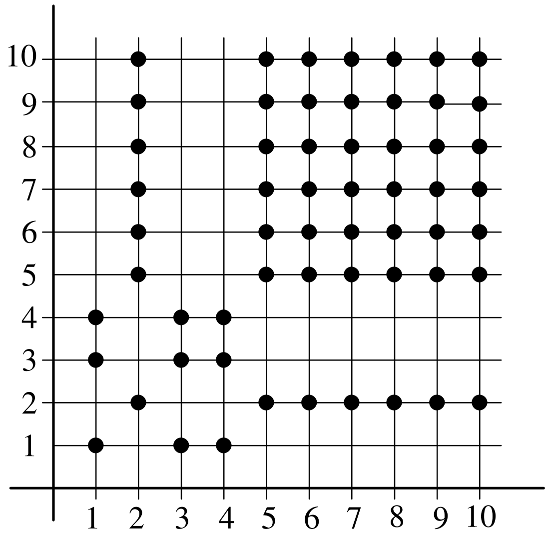
$$B_1 = \{1, 10\},\ B_2 = \{3, 4, 5\},\ B_3 = \{6, 7, 8, 9\},\ B_4 = \{2\}\ .$$

Rozklad A_1, A_2 určuje ekvivalenciu P na A, rozklad B_1, B_2, B_3, B_4 ekvivalenciu Q na A. Ich triedy ekvivalencie sú:

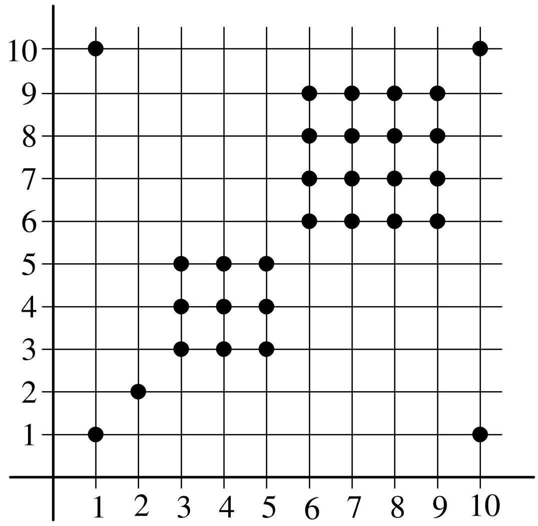
$$P(1) = \{1,2,3,4\},\ P(5) = \{5,6,7,8,9,10\};$$

$$Q(1) = \{1,10\},\ Q(4) = \{3,4,5\},\ Q(9) = \{6,7,8,9\},\ Q(2) = \{2\}.$$

Nakreslíme grafy relácií P, Q (obr. 20, 21). ■



Obr. 20. Graf ekvivalencie P



Obr. 21. Graf ekvivalencie Q

Budeme sa zaoberať reláciou ekvivalencie mod 3 na množine $\mathbf{Z}$. Triedy ekvivalencie sú

$$P(0) = \{3k; k \in \mathbf{Z}\},\ P(1) = \{3k+1; k \in \mathbf{Z}\},\ P(2) = \{3k+2; k \in \mathbf{Z}\}.$$

Na množine $\mathbf{Z}$ máme definovaný súčet čísel. Budeme zisťovať, aký je vzťah medzi triedami, v ktorých sú sčítance a kde je ich súčet. Nech ten súčet je, napríklad $6+2$. Vieme, že $6 \in P(0)$, $2 \in P(2)$ a pre súčet platí $P(6+2) = P(8) = P(2)$.

Zoberme ľubovoľné číslo $a \in P(0)$ a ľubovoľné $b \in P(2)$. Určíme $P(a+b)$, triedu, ktorej prvkom je číslo $a+b$.

Vieme, že $a = 3k$, $b = 3l+2$, $k, l \in \mathbf{Z}$. Potom $a+b = 3(k+l)+2$, kde $k+l \in \mathbf{Z}$, čo znamená $a+b \in P(2)$. Pretože $a+b \in P(a+b)$ aj $a+b \in P(2)$, tak $P(a+b) = P(2)$. Teda súčet ľubovoľného čísla z $P(0)$ a ľubovoľného čísla z $P(2)$ bude vždy prvkom $P(2)$. Symbolicky to zapíšeme $P(0)+P(2) = P(2)$.

Triedy $P(0)$, $P(2)$ tu neboli výnimkou, táto vlastnosť platí pre ľubovoľné dvojice z $P(0)$, $P(1)$, $P(2)$. Uvedieme symbolické zápisy výsledkov:

$$P(0)+P(0) = P(0+0) = P(0) \qquad P(1)+P(1) = P(1+1) = P(2)$$

$$P(0)+P(1) = P(0+1) = P(1) \qquad P(1)+P(2) = P(1+2) = P(0)$$

$$P(0)+P(2) = P(0+2) = P(2) \qquad P(2)+P(2) = P(2+2) = P(1)$$

Pretože v $\mathbf{Z}$ platí $a+b = b+a$, tak platí aj $P(a)+P(b) = P(b)+P(a)$.

Predchádzajúci princíp mám umožnil „preniesť“ súčet čísel zo $\mathbf{Z}$ na triedy ekvivalencie P, alebo, ináč povedané, definovať binárnu operáciu + na triedach ekvivalencie pomocou + na prvkoch **Z**. Vzhľadom na názornosť označujeme obidve operácie na **Z** aj na triedach ekvivalencie rovnako, aj keď sú to rôzne operácie na rôznych množinách.

Poznamenajme, že pomocou súčtu + na **Z** sa dá analogicky definovať binárna operácia na triedach ekvivalencie $\mathrm{mod}\, m$ pre každé $m \in \boldsymbol{N}^+$. Zdôvodníme to.

Nech $m \in \boldsymbol{N}^+$ je pevne určené číslo. Označme $P = \mathrm{mod}\, m$. Nech $c, d \in \mathbf{Z}$. Vieme, že $c \in P(c)$, $d \in P(d)$, $c + d \in P(c + d)$. Nech $a \in P(c)$, $b \in P(d)$ sú ľubovoľné prvky. Potom z definície relácie P platí:

$$c - a = k \,.\, m, \quad d - b = l \,.\, m, \quad k, l \in \mathbf{Z}$$

a teda c, a majú rovnaký zvyšok r po delení m a tiež b, d majú rovnaký zvyšok s po delení m. Teda platí

$$a = k_1 \,.\, m + r, \ c = k_2 \,.\, m + r, \ \text{kde } k_1, k_2 \in \mathbf{Z}, \ 0 \le r < m,$$
$$b = l_1 \,.\, m + s, \ d = l_2 \,.\, m + s, \ \text{kde } l_1, l_2 \in \mathbf{Z}, \ 0 \le s < m.$$

Nech zvyšok po delení $r + s$ číslom m je t, t.j.

$$r + s = nm + t, \ \text{kde } n \in \mathbf{Z}, \ 0 \le t < m.$$

Potom

$$c + d = (k_2 + l_2 + n)m + t, \ a + b = (k_1 + l_1 + n)m + t,$$

teda $(c + d) - (a + b)$ je celočíselný násobok čísla m, čo znamená $a + b \in P(c + d)$. Čiže súčet ľubovoľného prvku $a \in P(c)$ a ľubovoľného prvku $b \in P(d)$ vždy bude prvkom tej istej triedy $P(c + d)$. Symbolicky to zapíšeme $P(c) + P(d) = P(c + d)$.

Podobne môžeme „preniesť“ na triedy ekvivalencie $\mathrm{mod}\, m$ súčin čísel zo **Z**. Ak to má byť možné, tak pre každé dve triedy ekvivalencie $P(c)$, $P(d)$ a ľubovoľné $a \in P(c)$, $b \in P(d)$musí platiť $a \,.\, b \in P(c \,.\, d)$, tj. $P(a \,.\, b) = P(c \,.\, d)$. Použijeme rovnaké označenia ako v predchádzajúcich dvoch odsekoch.

Nech zvyšok po delení rs číslom m je v, teda

$$rs = n_1 m + v, \ n_1 \in \mathbf{Z}, \ 0 \le v < m.$$

Potom

$$cd = (k_2 m + r)(l_2 m + s) = (k_2 l_2 m + k_2 s + l_2 r)m + rs =$$
$$= (k_2 l_2 m + k_2 s + l_2 r + n_1)m + v = h_2 m + v$$
$$ab = (k_1 m + r)(l_1 m + s) = (k_1 l_1 m + k_1 s + l_1 r + n_1)m + v = h_1 m + v,$$

kde $h_1, h_2 \in \mathbf{Z}, \ 0 \le v < m$.

To znamená, že cd aj ab majú rovnaký zvyšok po delení m, teda $ab \in P(cd)$, čo sme chceli ukázať. Môžeme teda definovať binárnu operáciu násobenia (.) na množine tried ekvivalencie P, a to $P(c) \,.\, P(d) = P(c \,.\, d)$.

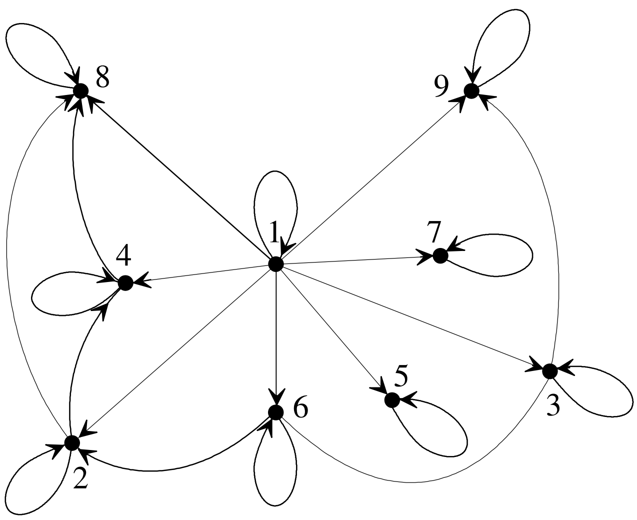
Relácia ekvivalencie na množine A, ktorá má tú vlastnosť, že na jej triedy ekvivalencie sa dajú preniesť operácie z A, patrí pod názov ***kongruencia*** na A. Nie je našou úlohou študovať pojem kongruencie, čitateľ sa s ním môže oboznámiť v každej matematickej knihe o algebrách, resp. algebraických štruktúrach. Chceli sme len ukázať princíp prenášania operácie na triedy.

Čiastočné usporiadanie na množine

Ak v definícii ekvivalencie zameníme symetrickosť za antisymetrickosť, dostaneme reláciu čiastočného usporiadania.

Relácia $P \subset A^2$, ktorá je reflexívna, antisymetrická a tranzitívna, sa nazýva ***reláciou čiastočného usporiadania*** na množine A, resp. ***čiastočným usporiadaním množiny*** A. Množina A spolu s reláciou P čiastočného usporiadania sa nazýva ***čiastočne usporiadaná množina*** a označuje sa (A, P).

Príklad. V predchádzajúcej časti o reláciách na množine sme ukázali, že relácia $\leq$ na množine **R** je reflexívna, antisymetrická, tranzitívna, teda je čiastočným usporiadaním množiny **R**. Potom $(\boldsymbol{R}, \leq)$ je čiastočne usporiadaná množina. ■



Obr. 22

Príklad. Definujme reláciu P na množine $\boldsymbol{N}^+$ takto: $(a, b) \in P$ práve vtedy, keď a delí b (označenie $a|b$), t.j. $b = k\,.\,a,\ k \in \boldsymbol{N}$.

Relácia | je reflexívna, lebo $a = 1\,.\,a$, teda $a|a$.

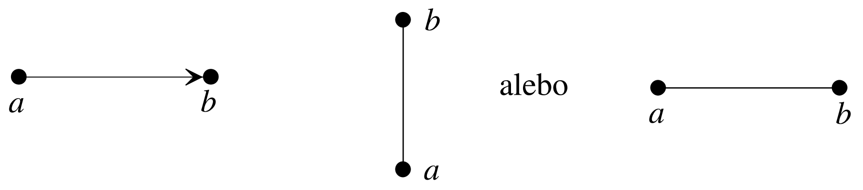
Relácia je antisymetrická, lebo z $a|b$ aj $b|a$ vyplýva $b = k\,.\,a,\ a = l\,.\,b,$ kde $k, l \in \boldsymbol{N}$. Potom $b = k\,.\,(l\,.\,b) = (k\,.\,l)\,.\,b,$ čiže $kl = 1$. Čísla k, l sú prirodzené, teda je jediná možnosť $kl = 1$, a to $k = 1, l = 1$, z čoho vyplýva $a = b$.

Relácia je tranzitívna, lebo z $a|b$, $b|c$ vyplýva $b = k\,.\,a,\ c = l\,.\,b,\ k, l \in \boldsymbol{N},$ čiže $c = (l\,.\,k)\,.\,a,$ $lk \in \boldsymbol{N},$ t.j. $a|c$.

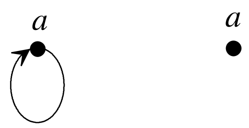
Dokázali sme, že relácia $|$ deliteľnosti na množine N^+ je čiastočným usporiadaním tejto množiny, teda $(N^+, |)$ je čiastočne usporiadaná množina. ■

Celý dôkaz môžeme zopakovať aj keď namiesto N^+ vezmeme jej ľubovoľnú podmnožinu $A \subset N^+$. Teda aj $(A, |)$ je čiastočne usporiadaná množina. Orientovaný graf tejto čiastočne usporiadanej množiny, kde $A = \{1, 2, ..., 10\}$, je na obr. 22.

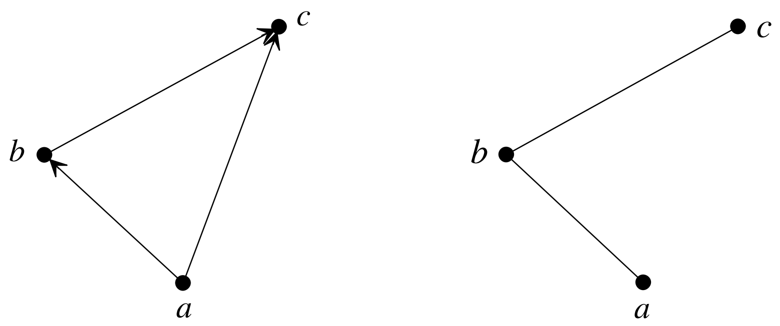
Vidíme, že orientovaný graf relácie je málo prehľadný už pri takomto malom počte prvkov množiny A. Aby sa orientované grafy čiastočne usporiadaných množín sprehľadnili, urobíme nasledovné dohody (pozri obr. 23, 24 a 25):



Obr. 23. Vynechanie šípiek



Obr. 24. Vynechanie slučiek



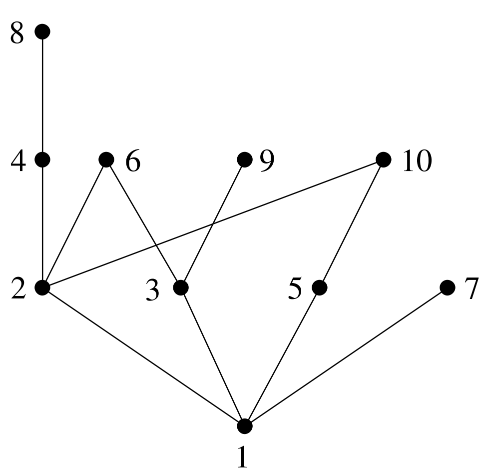
Obr. 25. Vynechanie hrany, ktorú zaručuje tranzitívnosť

Takto prekreslený orientovaný graf čiastočne usporiadanej množiny nazývame ***Hasseho diagram*** (krátko ***diagram***) ***čiastočne usporiadanej množiny***.

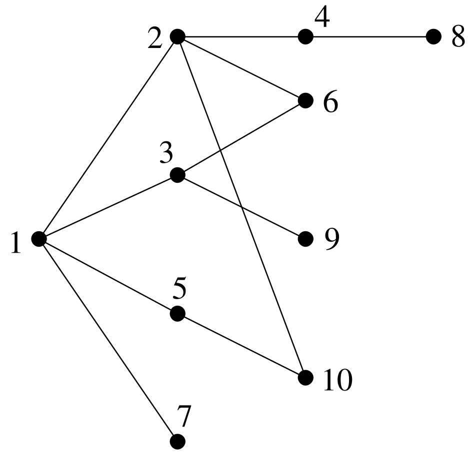
Diagram čiastočne usporiadanej množiny $(A, |)$, $A = \{1, 2, ..., 10\}$ je na obr. 26.

Nech P je relácia čiastočného usporiadania na množine A. Prvky $a, b \in A$ sa nazývajú ***porovnateľné*** v relácii P, ak aPb alebo bPa. Ak prvky a, b nie sú porovnateľné, tak sa nazývajú ***neporovnateľné*** v relácii P.

Ak je zrejmé o ktorú reláciu ide, tak vynechávame reláciu P a hovoríme len o porovnateľných a neporovnateľných prvkoch.



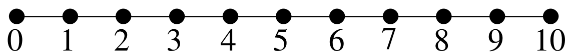
resp.



Obr. 26

Príklad. Prvky 4 a 8 z predchádzajúceho príkladu sú porovnateľné, prvky 6 a 8 sú neporovnateľné. Neporovnateľné sú aj prvky 5 a 4, porovnateľné sú 1 a 10. ■

Príklad. Nakreslite diagram čiastočne usporiadanej množiny $(A, \leq)$, kde $A = \{0, 1, ..., 10\}$.



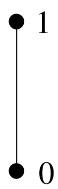
Obr. 27

Každé dva prvky sú tu porovnateľné. ■

Čiastočne usporiadaná množina (A, P), kde každé dva prvky sú porovnateľné, sa nazýva ***lineárne usporiadaná množina*** alebo ***reťazec***.

Nech **B** je dvojprvková množina, $\boldsymbol{B} = \{0, 1\}$. Definujeme na nej čiastočné usporiadanie σ pomocou Hasseho diagramu na obr. 28.

Množina **B** spolu s usporiadaním σ tvorí dvojprvkový reťazec. Tento reťazec sa nazýva dvojprvková Booleova algebra - skrátene ***Booleova algebra.*** Budeme ju označovať $\mathcal{B} = (\boldsymbol{B}, \sigma)$.



Obr. 28

Poznamenajme, že existujú Booleove algebry s viac ako dvoma prvkami. S týmito sa z pohľadu Boleových algebier nezaoberáme.

Príklad. Nech A je systém všetkých podmnožín množiny $X \neq \emptyset$. Potom inklúzia $\subset$ je reláciou čiastočného usporiadania na množine A.

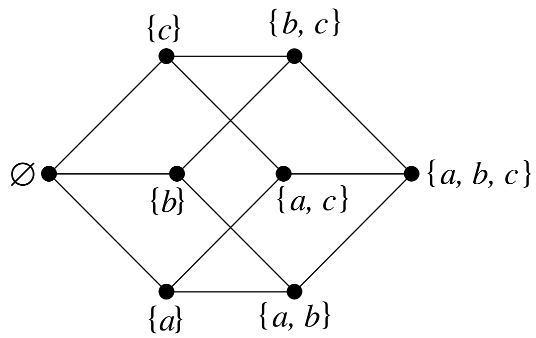
Pre každé $M \in A$ platí $M \subset M$, teda relácia je reflexívna.

Ak $M \subset S$ aj $S \subset M$, tak platí $M = S$, čiže relácia je antisymetrická.

Ak $M \subset S, S \subset T$ tak platí $M \subset T$, čiže relácia je tranzitívna.

Ukázali sme, že $(A, \subset)$ je čiastočne usporiadaná množina. Ak A je aspoň dvojprvková, tak to nie je reťazec, pretože pre dva rôzne prvky $a, b \in X$ sú množiny $\{a\}, \{b\}$ neporovnateľné prvky v relácii $\subset$.

Nech $X = \{a, b, c\}$. Potom diagram čiastočne usporiadanej množiny $(A, \subset)$ je uvedený na obr. 29. ■



Obr. 29

Cvičenia

1. Nakreslite graf a orientovaný graf relácie P na množine A, keď

a) $A = \{1, 2, ..., 10\},\ P = \{(1,2), (3,5), (2,2), (5,3), (8,9)\}$,

b) $A = \{a, b, c\},\ P = \{(a,a), (a,b), (b,c), (c,a), (a,c)\}$.

2. Zistite, či relácia P na množine A je reflexívna, symetrická, antisymetrická, tranzitívna, ak

a) $A = \boldsymbol{R}$ a platí xPy práve vtedy, keď $2x = 3y$,

b) $A = \boldsymbol{R}$ a platí xPy práve vtedy, keď $x \geq y, x \neq y$,

c) $A = \boldsymbol{R}$ a platí xPy práve vtedy, keď $|x| \leq |y|$,

d) $A = \boldsymbol{R}$ a platí xPy práve vtedy, keď $x \leq y$ alebo $x = 3y$,

e) $A = \boldsymbol{R}^+$ a platí xPy práve vtedy, keď $x = \frac{1}{y}$,

f) $A = \boldsymbol{R}^-$ a platí xPy práve vtedy, keď $x^2 + y^2 = 1$,

g) A je množina všetkých priamok v rovine a relácia P je relácia kolmosti $\perp$,

h) A je množina všetkých racionálnych čísel a relácia P je na A definovaná takto: $\frac{p}{q} P \frac{a}{b}$ práve vtedy, keď $pb = aq$. Poznamenajme, že táto relácia sa nazýva rovnosť zlomkov.

3. Zistite, či relácia P na množine $\boldsymbol{N}^+$ je ekvivalencia alebo čiastočné usporiadanie, keď

a) xPy práve vtedy, ak $y - x = 0$,

b) xPy práve vtedy, keď $x - y = 2$,

c) xPy práve vtedy, keď x, y sú nesúdeliteľné,

d) xPy práve vtedy, keď $x = y^2$.

4. Koľko rôznych relácií ekvivalencie je možné definovať na množine A, ak
a) $A = \{1, 2\}$,
b) $A = \{1, 2, 3\}$?

5. Na množine M všetkých štvorcových matíc stupňa n definujeme reláciu ~ takto:
$X \sim Y$ práve vtedy, keď existuje regulárna matica $D \in M$ tak, že $Y = D^{-1}XD$. Zistite, či táto relácia je ekvivalencia alebo čiastočné usporiadanie.

6. Zistite, či relácia P na množine A je reláciou ekvivalencie. Ak áno, nájdite jej triedy ekvivalencie, pričom
a) $A = \{1, 2, ..., 10\}$, a platí xPy práve vtedy, keď 2 delí $x + y$,
b) $A = \boldsymbol{N}^{+}$ a xPy práve vtedy, keď x delí y alebo y delí x,
c) $A = \boldsymbol{R}$ a xPy práve vtedy, keď $y - x$ je celé číslo.