# 2 Základy teórie množín

## 2.1 Základné pojmy

Je pozoruhodné, ako veľa matematických pojmov je možné vyjadriť pomocou množín a rozličných množinových konštrukcií. Je to nielen pozoruhodné, ale aj prekvapivé, lebo teória množín a dokonca i samotný pojem množiny sú zaradené do matematiky vlastne nedávno a ešte pred 100 rokmi bola teória odmietaná i niektorými poprednými vedcami. Dnes sa však teória množín stala súčasťou bežného matematického vyjadrovania, stala sa jazykom matematiky (a matematikov). Jazyk teórie množín napomohol chápať súčasnú matematiku pri všetkej jej rôznorodosti ako jeden celok majúci spoločné základy.

Teória množín je postavená na dvoch základných pojmoch „množina“ a „byť prvkom množiny“. Pod množinou si predstavujeme súbor objektov, ktoré majú nejakú spoločnú vlastnosť. Množiny budeme označovať veľkými písmenami $A$, $B$, $C$, $\ldots$, prípadne veľkými písmenami s indexami $A_1$, $A_2$, $\ldots$, $A_n$, $\ldots$.

Objekty, ktoré tvoria množinu nazývame prvkami danej množiny. Prvky množiny označujeme malými písmenami a v prípade potreby ich tiež indexujeme. Skutočnosť, že prvok $x$ patrí do množiny $A$ zapisujeme symbolicky $x \in A$ a hovoríme, že prvok $x$ je *elementom množiny* $A$. Ak $x$ nie je prvkom $A$, zapisujeme to: $x \notin A$ alebo $\neg(x \in A)$.

Zadať množinu možno v podstate dvomi spôsobmi a to buď vymenovaním jej prvkov (ak množina obsahuje konečný a nie príliš veľký počet prvkov), alebo charakterizáciou jej prvkov pomocou nejakej spoločnej vlastnosti. Tri bodky v zápise množiny znamenajú „a ďalej podobne podľa rovnakej zákonitosti“ (zákonitosť by mala byť zrejmá na prvý pohľad).

Pre niektoré nekonečné číselné množiny je zaužívané značenie: $\mathbb{N}$ – množina prirodzených čísel, $\mathbb{Z}$ – množina celých čísel, $\mathbb{Q}$ – množina racionálnych čísel, $\mathbb{R}$ – množina reálnych čísel, $\mathbb{C}$ – množina komplexných čísel.

Viacnásobný výskyt toho istého prvku v množine sa ignoruje (berie sa do úvahy len jeden výskyt).

**Príklad 2.1.** $A_1 = \{1, 2, 3, 4, 5\}$; $A_2 = \{x \mid (x \in \mathbb{Z}) \wedge (x > 5)\}$; $A_3 = \{x \mid (x \in \mathbb{N}) \wedge (x \text{ je deliteľné dvoma})\}$, $A_1 = \{1, 2, 3, 4, 5\} = \{2, 3, 3, 4, 3, 1, 5\}$; $A_4 = \{2, 4, 6, 8, \ldots\}$; $A_5 = \{2^1, 2^2, 2^3, \ldots\}$.

Ak zovšeobecníme prechádzajúce príklady vidíme, že množiny možno zadať nasledujúcim spôsobom:

$$A = \{x \mid P(x)\},$$

ktorý označuje, že $A$ je množina všetkých tých prvkov, ktoré majú vlastnosť $P$ a neobsahuje žiadne prvky, ktoré nemajú vlastnosť $P$.

Nekládli sme žiadne podmienky na to, aké objekty môžu byť prvkami množín. To znamená, že množiny môžu byť prvkami iných množín, napr.

$$x \in \{x\}, \quad \{x\} \in \{\{x\}\}, \quad x \in \{\{\{x\}\}, x\}.$$

Ako sa ukázalo začiatkom storočia, ak sa používa pojem množiny celkom slobodne a bez obmedzení, môže dôjsť k rôznym podivným situáciam, tzv. paradoxom.

**Príklad 2.2.** Paradox holiča: vojenský holič má holiť všetkých vojakov, ktorí sa neholia sami — má sa tento holič, ako jeden z vojakov holiť alebo nie?



**Príklad 2.3.**(Russellov paradox) Nech $\{1\}$ je jednoprvková množina obsahujúca číslo 1. Zrejme $1 \neq \{1\}$, a teda ani $\{1\} \notin \{1\}$. To znamená, že existuje množina $X$, ktorá má vlastnosť $P$: $X$ nie je prvkom seba samej. Vlastnosť $P$ je na prvý pohľad rozumná, možno ju ale použiť na definovanie množiny?

Skúsme vytvoriť množinu všetkých množín, ktoré majú vlastnosť $P$:

$$M = \{X \mid X \notin X\}.$$

Je zrejmé, že do $M$ patria všetky nám zatiaľ známe množiny: $\mathbb{N}$, $A_1, \ldots$. Čo však samotná množina $M$? Sú dve možnosti: buď $M \in M$, alebo $M \notin M$.

Nech $M \in M$. Množina $M$ je však „množinou“ všetkých množín $X$, pre ktoré platí $X \notin X$. Ak teda $M \in M$, nutne musí platiť $M \notin M$ a to je spor.

Skúsime druhú možnosť. Nech $M \notin M$. Potom podľa definície $M$ ($M$ obsahuje všetky množiny $X$ s vlastnosťou $X \notin X$) musí platiť $M \in M$ a to je opäť spor s predpokladom. To znamená, že súbor množín s vlastnosťou $P$ nemôže byť množina.

Vyhnúť sa Russelovmu paradoxu, či iným problémom a nejasnostiam vyplývajúcim z intuitívneho pojmu množiny možno pomocou axiomatickej výstavby teórii množín. Toto však nebude náš smer. Ale pre ukľudnenie duše, v našom výklade budú množiny rozumné a postupy na vytváranie množín nám budú vytvárať len množiny.

Počet prvkov, alebo mohutnosť množiny $X$ budeme označovať symbolom $|X|$. Cudzím slovom sa mohutnosti hovorí tiež *kardinalita*. Mohutnosť sa definuje aj pre nekonečné množiny.

## 2.2 Základné množinové vzťahy a operácie

**Definícia 2.4.** Nech $A$, $B$ sú ľubovoľné množiny. Hovoríme, že množina $A$ sa *rovná* množine $B$ (označujeme $A = B$) práve vtedy, ak každý prvok množiny $A$ je súčasne prvkom množiny $B$ a každý prvok množiny $B$ je súčasne prvkom množiny $A$.

Symbolicky zapísané:

$$\begin{aligned} A = B \;&\stackrel{\text{def}}{\equiv}\; \forall x\, [[(x \in A) \Rightarrow (x \in B)] \wedge [(x \in B) \Rightarrow (x \in A)]], \text{ resp.} \\ &\stackrel{\text{def}}{\equiv}\; \forall x\, [(x \in A) \equiv (x \in B)]. \end{aligned}$$

**Definícia 2.5.** Nech $A$, $B$ sú ľubovoľné množiny. Ak pre každý prvok $x \in A$ platí, že $x$ je prvkom $B$, potom hovoríme, že množina $A$ je *podmnožinou* množiny $B$, čo symbolicky zapisujeme $A \subseteq B$.

Ak $A \subseteq B$ a existuje prvok množiny $B$ taký, ktorý nepatrí do množiny $A$ (t.j. neplatí $B \subseteq A$), hovoríme, že $A$ je *vlastná podmnožina* množiny $B$, čo zapisujeme $A \subset B$.

Formálny zápis vzťahu $A \subseteq B$ vyzerá nasledujúco:

$$A \subseteq B \stackrel{\text{def}}{\equiv} \forall x\, [(x \in A) \Rightarrow (x \in B)].$$

Z porovnania predchádzajúcich dvoch definícií vidíme, že rovnosť množín $A$ a $B$ možno zapísať aj pomocou vzťahu inklúzie:

$$A = B \equiv ((A \subseteq B) \wedge (B \subseteq A)).$$

V ďalšom budeme predpokladať, že množiny, s ktorými pracujeme tvoria podmnožiny nejakej univerzálnej množiny $U$. Niektoré vzťahy medzi podmnožinami a množinové operácie možno veľmi efektívne reprezentovať pomocou tzv. Vennových diagramov.

**Definícia 2.6.** Nech $A$ a $B$ sú ľubovoľné množiny. *Zjednotením* množín $A$, $B$ nazveme množinu všetkých prvkov, ktoré patria aspoň do jednej z množín $A$, $B$:

$$A \cup B = \{x \mid (x \in A) \vee (x \in B)\}.$$

**Definícia 2.7.** Nech $A$ a $B$ sú ľubovoľné množiny. *Prienikom* množín $A$, $B$ nazveme množinu všetkých prvkov, ktoré patria súčasne do oboch množín $A$, $B$:

$$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}.$$

Čo v prípade, keď množiny $A$, $B$ nemajú spoločný prvok. Možno takúto „množinu“ považovať za množinu? Samozrejme, že áno. Jedná sa o tzv. prázdnu množinu.

**Definícia 2.8.** *Prázdna množina* je množina, ktorá neobsahuje žiaden prvok. Označujeme ju symbolom $\emptyset$ alebo $\{\}$.

**Príklad 2.9.** Prázdnu množinu možno definovať pomocou ľubovoľnej nesplniteľnej podmienky, napr.:

$$\begin{aligned} \emptyset &= \{x \mid x \in \mathbb{N} \wedge x < 0\}, \\ \emptyset &= \{x \mid x \neq x\}, \\ \emptyset &= \{x \mid x \in \mathbb{R} \wedge \sin x > 1\}. \end{aligned}$$

Dve množiny, ktorých prienikom je prázdna množina sa nazývajú *disjunktnými*.

**Veta 2.10.** (a) Prázdna množina je podmnožinou ľubovoľnej množiny.
(b) Existuje práve jedna prázdna množina.

DÔKAZ. Tvrdenie (a) dokážeme sporom. Predpokladajme, že tvrdenie (a) vety neplatí. To znamená, že platí negácia tohoto tvrdenia:

$$\neg \forall X\ (\emptyset \subseteq X); \text{t.j. } \exists X\ \neg(\emptyset \subseteq X),$$

čiže existuje taká množina $X$, že $\emptyset$ nie je podmnožinou $X$. Ale to znamená, že množina $\emptyset$ musí obsahovať prvok, ktorý nepatrí do $X$. To však nie je možné, lebo $\emptyset$ neobsahuje žiaden prvok. Dostali sme spor a to znamená, že predpoklad $(\neg \forall X\ (\emptyset \subseteq X))$ neplatí, ale platí jeho negácia $\forall X\ (\emptyset \subseteq X)$, čo sme mali dokázať.

Pri dôkaze tvrdenia (b) budeme postupovať taktiež sporom. Nech teda existujú dve rozličné prázdne množiny $B_1$, $B_2$. Využijeme dokázané tvrdenie (a). Keďže obe množiny $B_1$ a $B_2$ sú prázdne, podľa (a) platí $B_1 \subseteq B_2$, ale aj $B_2 \subseteq B_1$. Z toho vyplýva, že $B_1 = B_2$. To znamená, že ľubovoľné dve prázdne množiny sa rovnajú, čo je spor s predpokladom existencie dvoch rôznych prázdnych množín. $\square$

**Definícia 2.11.** Nech $A$ je ľubovoľná množina, $A \subseteq U$. *Doplnkom* množiny $A$ vzhľadom na množinu $U$ nazývame množinu všetkých tých prvkov $U$, ktoré nepatria do množiny $A$:

$$A^c = \{x \mid x \in U \wedge \neg(x \in A)\}.$$

Keď uvažujeme doplnok vzhľadom na univerzálnu množinu $U$, často používame skrátený zápis $A^c = \{x \mid x \notin A\}$. Doplnok množiny možno vyjadriť nielen vzhľadom na univerzálnu, ale aj vzhľadom na ľubovoľnú množinu. Na to nám slúži ďalšia množinová operácia – rozdiel množín.



**Definícia 2.12.** Nech $A$, $B$ sú ľubovoľné množiny. *Rozdielom* množín $A$, $B$ nazveme množinu všetkých tých prvkov množiny $A$, ktoré nepatria do $B$:

$$A \setminus B = \{x \mid x \in A \wedge \neg(x \in B)\}.$$

Rozdiel množín môžeme vyjadriť pomocou prieniku a doplnku nasledovne:

$$A \setminus B = A \cap B^c.$$

Doplnok $A^c$ nie je teda nič iné, ako $U \setminus A = U \cap A^c$.

**Definícia 2.13.** Nech $A$, $B$ sú ľubovoľné množiny. *Symetrickou diferenciou* množín $A$, $B$ nazveme množinu

$$A \doteq B = \{x \mid [(x \in A) \wedge \neg(x \in B)] \vee [(x \in B) \wedge \neg(x \in A)]\}.$$

Symetrickú diferenciu množín $A$, $B$ možno vyjadriť pomocou rozdielu a zjednotenia množín nasledovne:

$$A \doteq B = (A \setminus B) \cup (B \setminus A).$$

## 2.3 Základné množinové identity

Tú istú množinu možno vyjadriť rozličnými spôsobmi pomocou iných množín. Je pochopiteľné, že sa budeme snažiť získať vyjadrenie množiny v čo najjednoduchšom tvare. Na to budeme využívať množinové identity vychádzajúce z vlastností množinových operácií.

**Veta 2.14.** Nech $A$, $B$, $C$ sú ľubovoľné množiny. Potom platí:

i. $A \cup A = A$, $A \cap A = A$ (idempotentnosť)
ii. $A \cup B = B \cup A$, $A \cap B = B \cap A$ (komutatívnosť)
iii. $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$ (asociatívnosť)
iv. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (distributívne zákony)
v. $A \subseteq A \cup B$, $B \subseteq A \cup B$, $A \cap B \subseteq A$, $A \cap B \subseteq B$
vi. $(A \cup B)^c = (A^c \cap B^c)$, $(A \cap B)^c = (A^c \cup B^c)$ (de Morganove zákony)
vii. $(A^c)^c = A$
viii. $A \cap \emptyset = \emptyset$, $A \cup \emptyset = A$
ix. $A \cap A^c = \emptyset$, $A \cup A^c = U$
x. $A \cap (A \cup B) = A$, $A \cup (A \cap B) = A$ (absorpčné zákony)

DÔKAZ. Vo všetkých prípadoch možno použiť priamy dôkaz podľa nasledujúcej schémy, v ktorej dokážeme platnosť jedného z asociatívnych zákonov (iii):

1. $x \in A \cup (B \cup C)$

2. $(x \in A) \vee x \in (B \cup C)$

3. $(x \in A) \vee [(x \in B) \vee (x \in C)]$

4. $[(x \in A) \vee (x \in B)] \vee (x \in C)$ disjunkcia je asociatívna logická operácia

5. $x \in (A \cup B) \vee (x \in C)$

6. $x \in (A \cup B) \cup C$

Na výber prvku $x$ sme nekládli žiadne obmedzenia. Z toho vyplýva, že každý prvok z $A \cup (B \cup C)$ patrí aj do $(A \cup B) \cup C$. Naviac pri dôkaze sme používali len ekvivalentné úpravy výrokov a tým sme dokázali aj tvrdenie, že každý prvok z $(A \cup B) \cup C$ patrí do množiny $A \cup (B \cup C)$. Dokázali sme teda, že

$$\begin{aligned} A \cup (B \cup C) &\subseteq (A \cup B) \cup C \text{ a} \\ (A \cup B) \cup C &\subseteq A \cup (B \cup C), \text{ čiže} \\ (A \cup B) \cup C &= A \cup (B \cup C). \end{aligned}$$

Zhrnieme celý postup: vybrali sme ľubovoľný prvok $x$ z množiny ležiacej na ľavej strane identity. Využili sme definície množinových operácií a výrok „$x$ patrí do zloženej množiny" sme rozpísali na zložený výrok o príslušnosti $x$ do množín $A$, $B$. Tento zložený výrok sme upravili využívajúc poznatky z výrokovej logiky (ekvivalentné úpravy). Zložený výrok sme potom, použijúc definície množinových operácií, upravili na výrok o príslušnosti prvku do „zloženej" množiny z pravej strany identity. Ak sme pri úpravách výrokov použili ekvivalentné úpravy, dokázali sme týmto rovnosť množín; ak sme použili neekvivalentné úpravy, dokázali sme len množinovú inklúziu.

Dôkaz (iv):

1. $[x \in A \cap (B \cup C)] \equiv [(x \in A) \wedge x \in (B \cup C)]$,

2. $[(x \in A) \wedge x \in (B \cup C)] \equiv [(x \in A) \wedge ((x \in B) \vee (x \in C))]$,

3. $[(x \in A) \wedge ((x \in B) \vee (x \in C))] \equiv [((x \in A) \vee (x \in B)) \wedge ((x \in A) \vee (x \in C))]$

4. $[((x \in A) \vee (x \in B)) \wedge ((x \in A) \vee (x \in C))] \equiv [(x \in A \cup B) \wedge (x \in A \cup C)]$,

5. $[(x \in A \cup B) \wedge (x \in A \cup C)] \equiv [x \in (A \cup B) \cap (x \in A \cup C)]$.

V krokoch 1, 2, 4 a 5 sme použili definíciu prieniku a zjednotenia, v kroku 3, ktorý je kľúčový pre dôkaz identity, sme využili distributívny zákon pre konjunkciu a disjunkciu z výrokovej logiky.

Dokážeme inklúziu (v). Využijeme tautológiu $p \Rightarrow (p \vee q)$. Predpokladáme, že

1. $x \in A$,

2. $(x \in A) \Rightarrow [(x \in A) \vee (x \in B)]$, (využitie tautológie $p \Rightarrow (p \vee q)$),

3. $[(x \in A) \vee (x \in B)] \equiv x \in (A \cup B)$,

4. $(x \in A) \Rightarrow (x \in A \cup B)$ (pravidlo sylogizmu).



Pretože tvrdenie platí pre ľubovoľné $x$, dostávame

$$A \subseteq A \cup B.$$

Dôkaz nemožno otočiť, v druhom riadku je namiesto ekvivalencie implikácia. □

V nasledujúcej vete uvedieme niektoré vlastnosi rozdielu množín.

**Veta 2.15.** Nech $A$, $B$, $C$ sú ľubovoľné množiny, potom platia nasledujúce vzťahy:

i. $(A \cap B) \setminus C = A \cap (B \setminus C)$,

ii. $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$,

iii. $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$,

iv. $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$, (de Morganove pravidlá)

v. $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$,

vi. $A \setminus B = A \setminus (A \cap B) = (A \cup B) \setminus B$,

vii. $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$,

viii. $(A \setminus B) \setminus C = A \setminus (B \cup C)$.

DÔKAZ. Pri dôkazov týchto identít využijeme už dokázané množinové identity. Ekvivalentnými úpravami sa snažíme jednu stranu identity upraviť na výraz ležiaci na druhej strane. Pri úpravách najprv nahradíme rozdiel množín $X \setminus Y$ prienikom $X \cap Y^c$. Ak $Y$ je v tvare zjednotenia alebo prieniku množín, využijeme de Morganove zákony a upravíme výraz na taký tvar, v ktorom vystupujú už len doplnky „jednoduchých" množín. Potom použijeme distributívny zákon, využijeme asociatívny, komutatívny a absorpčný zákon, resp. zákon idempotentnosti a upravíme na potrebný tvar:

Dôkaz (iv):

$$\begin{aligned} (C \setminus A) \cup (C \setminus B) &= (C \cap A^c) \cup (C \cap B^c) = C \cap (A^c \cup B^c) = C \cap (A \cap B)^c \\ &= C \setminus (A \cap B). \end{aligned}$$

Dôkaz (viii):

$$\begin{aligned} (A \setminus B) \setminus C &= (A \cap B^c) \cap C^c = A \cap (B^c \cap C^c) = A \cap (B \cup C)^c \\ &= A \setminus (B \cup C). \end{aligned}$$

□

Pozrime sa teraz na základné vlastnosti symmetrickej diferencie množín:

**Veta 2.16.** Nech $A$, $B$, $C$ sú ľubovoľné množiny. Potom platia nasledujúce vzťahy:

i. $A \doteq B = B \doteq A$ (komutatívnosť)

ii. $A \dot{-} B = (A \cup B) \setminus (A \cap B)$,

iii. $A \dot{-} (B \dot{-} C) = (A \dot{-} B) \dot{-} C$, (asociatívnosť)

iv. Rovnica $X \dot{-} A = B$ má jediné riešenie $X = A \dot{-} B$.

DÔKAZ. (i) Vyplýva priamo z definície symetrickej diferencie.

Dôkaz (ii):

$$\begin{aligned}
(A \cup B) \setminus (A \cap B) &= (A \cup B) \cap (A \cap B)^c = (A \cup B) \cap (A^c \cup B^c) \\
&= [(A \cup B) \cap A^c] \cup [(A \cup B) \cap B^c] = [(A \cap A^c) \cup (B \cap A^c)] \cup [(A \cap B^c) \cup (B \cap B^c)] \\
&= [\emptyset \cup (B \cap A^c)] \cup [(A \cap B^c) \cup \emptyset] = (B \cap A^c) \cup (A \cap B^c) \\
&= (B \setminus A) \cup (A \setminus B) = A \dot{-} B.
\end{aligned}$$

(iv) Najskôr dokážeme, že množina $A \dot{-} B$ je riešením rovnice $X \dot{-} A = B$:

$$(A \dot{-} B) \dot{-} A = (B \dot{-} A) \dot{-} A = B \dot{-} (A \dot{-} A) = B \dot{-} \emptyset = B.$$

Teraz ukážeme, že riešenie $X = A \dot{-} B$ je jediné. Použijeme dôkaz sporom. Predpokladajme, že pre množinu $Y \neq A \dot{-} B$ platí $Y \dot{-} A = B$. Potom $Y = Y \dot{-} (A \dot{-} A) = (Y \dot{-} A) \dot{-} A = B \dot{-} A$ a to je hľadaný spor. $\square$

Máme už dosť široký repertoár množinových identít a isté skúsenosti s dokazovaním rovnosti množín. Na dokázanie toho, že dve množiny sú vo vzťahu inklúzie však doposiaľ musíme namáhavo dokazovať, že každý prvok prvej množiny je súčasne prvkom druhej množiny. Nasledujúca veta ukazuje, ako možno previesť zisťovanie množinovej inklúzie na overenie, či sa dve množiny rovnajú:

**Veta 2.17.** Nech $A$, $B$ sú ľubovolné podmnožiny množiny $U$. Potom sú nasledujúce výroky ekvivalentné:

i. $A \subseteq B$,

ii. $A \cap B = A$,

iii. $A \cup B = B$,

iv. $A \setminus B = \emptyset$,

v. $A^c \cup B = U$,

vi. $A \dot{-} B = B \setminus A$.

DÔKAZ. Máme dokázať, že ľubovoľné tvrdenia sú ekvivalentné. V takýchto prípadoch sa zvyčajne dokáže, že (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (v) $\Rightarrow$ (vi) $\Rightarrow$ (i) a platnosť ostatných dostávame pomocou pravidla sylogizmu. Napríklad implikácia (ii) $\Rightarrow$ (vi) vyplýva z implikácií:

$$\frac{(ii) \Rightarrow (iii), (iii) \Rightarrow (iv), (iv) \Rightarrow (v), (v) \Rightarrow (vi)}{(ii) \Rightarrow (vi)}$$

a opačná implikácia z:

$$\frac{(vi) \Rightarrow (i), (i) \Rightarrow (ii)}{(vi) \Rightarrow (ii)} \quad \text{(sylogizmus).}$$



(i) $\Rightarrow$ (ii): Nech $A \subseteq B$. Potrebujeme dokázať dve inklúzie: $A \cap B \subseteq A$ a $A \subseteq A \cap B$. Prvá inklúzia platí pre ľubovoľné množiny $A$, $B$ (veta 2.3). Platnosť druhej inklúzie dokážeme sporom. Nech teda $A \subseteq B$, ale nech súčasne $\neg(A \subseteq A \cap B)$ (predpoklady).

Rozpíšme druhý predpoklad:

$$\begin{aligned}
\neg(A \subseteq A \cap B) &\equiv \neg\forall\,(x \in A \Rightarrow x \in A \cap B) \equiv \exists x\, \neg(x \in A \Rightarrow x \in A \cap B) \\
&\equiv \exists x\,(x \in A \wedge \neg(x \in A \cap B).
\end{aligned}$$

To znamená, že existuje prvok $a$, ktorý patrí do množiny $A$, ale nepatrí do množiny $A \cap B$; t.j.

$$\begin{aligned}
&(a \in A) \wedge \neg[(a \in A) \wedge (a \in B)] \equiv (a \in A) \wedge [\neg(a \in A) \vee \neg(a \in B)] \\
\equiv\ &[(a \in A \wedge \neg(a \in A)] \vee [(a \in A) \wedge \neg(a \in B)] \equiv [(a \in A) \wedge \neg(a \in B)].
\end{aligned}$$

Predpokladali sme však, že $A \subseteq B$, t.j. podľa definície inklúzie $\forall x\ (x \in A \Rightarrow x \in B)$ a teda aj pre prvok $a$ platí $(a \in A) \Rightarrow (a \in B)$. Tvrdenie, ktoré sme odvodili $[(a \in A) \wedge \neg(a \in B)]$ je negáciou tvrdenia $[(a \in A) \Rightarrow (a \in B)]$. Dostali sme spor, ktorý dokazuje, že za predpokladu $A \subseteq B$ musí platiť aj $A \subseteq A \cap B$.

(ii) $\Rightarrow$ (iii):

Predpokladáme, že platí $A \cap B = A$. Dokážeme platnosť tvrdenia $A \cup B = B$:

$$A \cup B = (A \cap B) \cup B = B$$

na základe absorpčného zákona. (iii) $\Rightarrow$ (iv):

Predpokladáme, že platí $A \cup B = B$. Potom

$$A \setminus B = A \setminus (A \cup B) = A \cap (A \cup B)^c = A \cap (A^c \cap B^c) = (A \cap A^c) \cap B^c = \emptyset.$$

(iv) $\Rightarrow$ (v):

Túto časť dokážeme sporom. Nech $A \setminus B = \emptyset$, ale $A^c \cup B \neq U$. Keďže $U$ je univerzálna množina, nutne existuje prvok $a$, ktorý patrí do $U$ ale nepatrí do $A^c \cup B$. To znamená, že $\neg((a \in A^c) \vee (a \in B)) \equiv \neg(\neg(a \in A) \vee (a \in B)) \equiv ((a \in A) \wedge \neg(a \in B)) \equiv [(a \in A) \wedge (a \in B^c)] \equiv [a \in A \cap B^c] \equiv a \in A \setminus B$. Keďže podľa predpokladu $A \setminus B = \emptyset$, prvok $a$ s uvedenou vlastnosťou nemôže existovať. Dospeli sme k sporu.

(v) $\Rightarrow$ (vi):

Predpokladáme, že platí $A^c \cup B = U$. Ak má platiť $(A \dot{-} B) = (B \setminus A)$, potom množina $A \setminus B$ musí byť prázdna, pretože vo všeobecnom prípade $(A \dot{-} B) = (A \setminus B) \cup (B \setminus A)$ a množiny $(A \setminus B)$ a $(B \setminus A)$ sú zrejme disjunktné. Predpokladajme, že množina $A \setminus B \neq \emptyset$. Potom existuje prvok $a \in A \setminus B$; t.j. $(a \in A) \wedge \neg(a \in B)$. Tento prvok nepatrí ani do množiny $A^c$, ani do množiny $B$, t.j. nemôže patriť ani do množiny $A^c \cup B$. Ale $A^c \cup B = U$, a to znamená, že $\neg(a \in U)$. Spor.

(vi) $\Rightarrow$ (i):

Opäť použijeme dôkazom sporom. Nech $A \dot{-} B = B \setminus A$ a súčasne $\neg(A \subseteq B)$. To znamená, že existuje prvok $a \in A$, ktorý nepatrí do $B$; t.j. $\neg(a \in B)$. Ale tento prvok patrí do množiny $A \setminus B$ (a nepatrí do množiny $B \setminus A$.) To znamená, že $A \dot{-} B \neq B \setminus A$. Spor. $\square$

**Poznámka.** Pri všetkých matematických tvrdeniach sú dôležité predpoklady, pri ktorých tvrdenia platia. Napríklad vo všeobecnom prípade platí: $(A \dot{-} B) = (A \setminus B) \cup (B \setminus A)$. Ak však pripustíme platnosť ďalších predpokladov, napríklad $A^c \cup B = U$, dokážeme $(A \dot{-} B) = (B \setminus A)$, ktorá však vo všeobecnom prípade neplatí.

**Veta 2.18.** Nech $A$, $B$, $C$ sú ľubovoľné množiny.
(a) Inklúzia $C \subseteq A \cap B$ platí práve vtedy, ak $C \subseteq A$ a $C \subseteq B$.
(b) Inklúzia $A \cup B \subseteq C$ platí práve vtedy, ak $A \subseteq C$ a $B \subseteq C$.

DÔKAZ. Vetu možno dokázať viacerými spôsobmi. Najskôr si však všimnime štruktúru jej tvrdení:
$p$ označuje výrok: $C \subseteq A \cap B$,
$q$ označuje výrok: $C \subseteq A$,
$r$ označuje výrok: $C \subseteq B$,
$s$ označuje výrok: $A$, $B$, $C$ sú ľubovoľné množiny
Potom tvrdenie možno schématicky zapísať takto:

$$\frac{s \text{ (predpoklad)}}{p \equiv (q \wedge r) \text{ (tvrdenia, ktor0 treba dokázať)}}.$$

Dokázať ekvivalenciu znamená dokázať konjunkciu dvoch implikácii, t.j.

$$(p \Rightarrow (q \wedge r)) \wedge ((q \wedge r) \Rightarrow p).$$

Prejdime k dôkazu tvrdenia (a). Implikáciu $(p \Rightarrow (q \wedge r))$ dokážeme sporom. Nech $C \subseteq A \cap B$ a $\neg(C \subseteq A \wedge C \subseteq B)$. To znamená, že platí tvrdenie $\neg(C \subseteq A) \vee \neg(C \subseteq B)$ a teda buď existuje prvok $a$, $a \in C \setminus A$ alebo $b \in C \setminus B$. Keďže $C \setminus A \subseteq C$, $C \setminus B \subseteq C$ a $C \subseteq A \cap B$, potom aj $C \setminus A \subseteq A \cap B$ a $C \setminus B \subseteq A \cap B$. Čo však s prvkom $a$ (resp. $b$)? Prvok $a$ nepatrí do $A$ a teda nepatrí ani do množiny $A \cap B$ (podobne pre prvok $b$). To znamená, že $C$ nemôže byť podmnožinou $A \cap B$. Spor.

Implikáciu $(q \wedge r) \Rightarrow p$ dokážeme priamo. Nech platí $C \subseteq A$ a $C \subseteq B$, To znamená, že $C \cap A = C$, $C \cap B = C$. Ale potom aj $(A \cap B) \cap C = A \cap (B \cap C) = A \cap C = C$, a teda $C \subseteq A \cap B$.

(b) Tvrdenie sa dokazuje analogicky. □

## 2.4 Potenčná množina

**Definícia 2.19.** Nech je daná množina $M$. *Potenčnou množinou* množiny $M$ nazveme množinu všetkých podmnožín množiny $M$:

$$\mathcal{P}(M) = \{X \mid X \subseteq M\}.$$

Potenčná množina sa niekedy označuje aj symbolom $2^M$.

**Príklad 2.20.** Nech $M = \{1,2\}$, potom $\mathcal{P}(M) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$.

**Veta 2.21.** Ľubovoľná $n$ prvková množina má práve $2^n$ podmnožín.

DÔKAZ. Dôkaz urobíme matematickou indukciou. Označme $X$ ľubovoľnú $n$ prvkovú množinu. Pre $X = \emptyset$ existuje jediná podmnožina, a to prázdna, čo súhlasí s počtom $2^0 = 1$. Ak máme $(n+1)$-prvkovú množinu $X$, zvoľme jeden jej prvok, $a$, a rozdeľme podmnožiny $X$ do dvoch typov: tie, ktoré neobsahujú $a$, a tie, ktoré ho obsahujú. Prvého typu sú práve všetky podmnožiny $n$-prvkovej množiny $X \setminus \{a\}$, a podľa indukčného predpokkladu ich je $2^n$. Pre každú podmnožinu $A$ druhého typu uvážme množinu $A = A \setminus \{a\}$. To je podmnožina $X \setminus \{a\}$. Zrejme každá podmnožina $A' \subseteq X \setminus \{a\}$ sa takto dostane práve z jednej množiny $A$, totiž z $A' \cup \{a\}$. Preto podmnožín $A$ druhého typu je tiež $2^n$, a celkom máme $2^n + 2^n = 2^{n+1}$ podmnožín $(n+1)$-prvkovej množiny, ako má byť. □



**Veta 2.22.** Nech $n \geq 1$. Každá $n$-prvková množina má práve $2^{n-1}$ podmnožín párnej veľkosti a $2^{n-1}$ podmnožín nepárnej veľkosti.

DÔKAZ. Označme $X$ ľubovoľnú $n$-prvková množinu. Zvoľme nejaký prvok $a \in X$. Ľubovoľnú podmnožinu $A \subseteq X \setminus \{a\}$ môžeme doplniť na podmnožinu $A' \subseteq X$ s nepárnym počtom prvkov: ak je $|A|$ nepárne, položme $A' = A$; ak je $|A|$ párne, položme $A' = A \cup \{a\}$. Je dôležité si uvedomiť, že sme tým našli bijekciu medzi množinou všetkých podmnožín $X$ nepárnej veľkosti a množinou všetkých podmnožín $X \setminus \{a\}$, ktorých je práve $2^{n-1}$ podľa predchádzajúcej vety.

Párnych podmnožín je doplnok do celkového počtu podmnožín, t.j. $2^{n-1}$. □